KinderGate
Parental Control

KinderGate Parental Control
Benutzerhandbuch

www.entensys.de

entensys

KinderGate Parental Control

Inhaltsverzeichnis

Einführung **4**

Über KinderGate **5**

KinderGate Features **6**

Filterungsmethoden **7**

Installation von KinderGate **8**
- Systemanforderungen 8
- Installation von KinderGate auf Linux-PC's 8
  - Für Ubuntu 12.04 8
  - Für Ubuntu 13.10 8
  - Für Ubuntu 14.04 8
  - Für Alt Linux 7 x32 8
- Installation von KinderGate für Mac OSX 8
- Installation von KinderGate unter MS Windows 10
- Ersteinrichtung und Registrierung 10
- Einfacher Installationsmodus 12
- Cluster-Installationsmodus 12

Lizenz für KinderGate registrieren **15**
- Testlizenz 15
- Vollwertige Lizenz 16

Updates für KinderGate **19**
- Software Update für Linux 19
  - Für Ubuntu und Alt Linux 19
- Software Update für Mac OSX 19
- Software Update für MS Windows 19

Deinstallation von KinderGate **20**
- Software-Deinstallation für Linux 20
  - Für Ubuntu und Alt Linux 20
- Software-Deinstallation für MS Windows 20
- Software-Deinstallation für Mac OSX 20

KinderGate Filtereinstellungen **21**
- Starten der KinderGate Konsole 21
- Einfache Admin-Konsole 21
- Erweiterte Admin-Konsole 23
  - Lizenz 25
  - Allgemeine Einstellungen 26
  - Morphologie 29
  - URL-Kategorien 34
  - Ausschlüsse 38
  - Sichere Verbindung 40
  - Anfragen 41
  - Login-Historie 43
  - Statistiken 44

Technischer Support **46**

Anhänge **47**
Anhang 1. Einrichtung eines lokalen Zertifizierungsstellen-Stammzertifikats 47
Einrichtung des Zertifikats für Internet Explorer und Chrome unter MS Windows 47
Einrichtung des Zertifikats für Safari und Chrome unter Mac OSX 52
Zertifikat in Firefox einrichten 53

Einführung

Das Programm KinderGate Parental Control (nachfolgend KinderGate) dient dazu, Internetaktivitäten zu kontrollieren und Minderjährige von gefährlichen oder schädlichen Webseiten und Ressourcen, die Gewalt, Extremismus, Drogen, Pornografie oder Selbstmord propagieren, sowie von unerwünschten Dating-Seiten, Foren usw. fernzuhalten.

KinderGate
Parental Control

Über KinderGate

Die Software-Lösung KinderGate filtert Webseiten, basierend auf ihren Inhalten und hindert den Zugriff auf einige Webseiten oder Internet-Dienste, indem die für Minderjährige unerwünschten Inhalte blockiert oder gesperrt werden. Es werden Adds, Pop-Up-Fenster, Banner sowie der Zugang zu sozialen Netzwerken und Videos blockiert.

KinderGate kann auf Schul- oder Privatrechnern installiert werden und bietet ein sicheres Surfen für Internetnutzer.

KinderGate Parental Control

KinderGate Features

Mit KinderGate können Sie schnell Filtereinstellungen für jede Internetverbindung mithilfe einer einfachen Admin-Konsole und komplexeren Filtern mit erweiterter Admin-Konsole festlegen. Es ist ebenfalls möglich, Statistiken der Internetaktivität und den Verbindungsstatus von Webseiten einzusehen.

Das Zuordnen und Blockieren von Seiten wird anhand der Textanalyse und Suche nach in Entensys eingebauten Wörterbücher mit Worten und Ausdrücken wie „Schlimme Wörter", „Drogen", „Glücksspiel", „Pornografie", „Selbstmord" oder „Terrorismus" kinderleicht.

Im Programm können eigenen Wörterbücher erstellt und mit Schlüsselwörtern ergänzt werden, die Einstellungen für Internetoptionen und Kategorien der zu blockierenden Webseiten festlegt, der Zugang zu Webseiten für jeden Nutzer verwaltet sowie verschiedene Internetressourcen erlaubt oder blockiert werden.

Die Software-Lösung ist ein effektiver und genauer Internetfilter, welcher den Zugang zu unbedenklichen Ressourcen nicht sperrt.

Filterungsmethoden

Das Programm KinderGate bietet sowohl URL- als auch eine Kategorie-Filterung. Sie verfügt über zahlreiche Methoden, Internetverkehr einzuschätzen und kann den Zugang zu gesamten Webseiten oder nur bestimmte Bereiche dieser blockieren, dank folgender HTTP-Filterungsmethoden:

- Nach Kategorie der Webseite (Entensys URL-Filterung 2.0);
- Morphologische Analyse und reguläre Ausdrücke;
- Überwachung von heruntergeladenen Dateien je nach Typ;
- Funktion der Sicheren Suche;
- Filterung von Kontextwerbung;
- White- und Blacklisten.

KinderGate Parental Control

Installation von KinderGate

Systemanforderungen

Wir empfehlen für die Installation von KinderGate MS Windows XP/Vista/Windows 7, Linux oder Macintosh OSX 10.7.5 oder höher, mit einem aktiven Internetanschluss, zu verwenden. Es sind mindestens 2 GB RAM und 200 MB Festplattenspeicher für einen effektiven Betrieb erforderlich.

Installation von KinderGate auf Linux-PC's

KinderGate wird aus einem Repositorium von Entensys heruntergeladen. Führen Sie bitte folgende Befehle aus, um die Anwendung zu installieren:

Für Ubuntu 12.04

echo 'deb http://dc.entensys.com/ubuntu precise extra' | sudo tee -a /etc/apt/sources.list
wget http://dc.entensys.com/ubuntu/entensys.gpg -O - | sudo apt-key add -
sudo apt-get update
sudo apt-get install kindergate

Für Ubuntu 13.10

echo 'deb http://dc.entensys.com/ubuntu saucy extra' | sudo tee –a /etc/apt/sources.list
wget http://dc.entensys.com/ubuntu/entensys.gpg -O - | sudo apt-key add -
sudo apt-get update
sudo apt-get install kindergate

Für Ubuntu 14.04

echo 'deb http://dc.entensys.com/ubuntu trusty extra' | sudo tee -a /etc/apt/sources.list
wget http://dc.entensys.com/ubuntu/entensys.gpg -O - | sudo apt-key add -
sudo apt-get update
sudo apt-get install kindergate

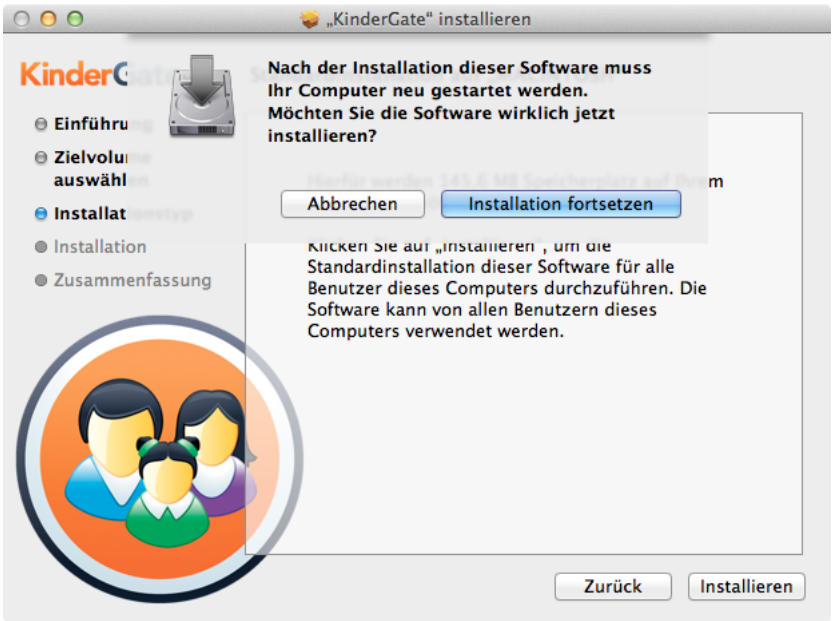
Für Alt Linux 7 x32

echo 'rpm http://dc.entensys.com/alt7 i686 extra' | sudo tee -a /etc/apt/sources.list
apt-get update
apt-get install kindergate

Installation von KinderGate für Mac OSX

KinderGate wird mit dem Ausführen der Installationsdatei installiert, ein Dialogfenster des Installationsassistenten öffnet sich. Folgen Sie den Installationsanweisungen des Assistenten.

Ist der Installationsvorgang abgeschlossen, starten Sie Ihren Rechner neu:



KinderGate wird standardmäßig unter /opt/entensys/kindergate installiert.

Installation von KinderGate unter MS Windows

KinderGate wird mit dem Ausführen der Installationsdatei installiert, ein Dialogfenster des Installationsassistenten öffnet sich.

Der Installationsassistent führt alle für die Installation von KinderGate notwendigen Vorgänge automatisch aus: Dateien werden ausgepackt, zusätzlicher Systemdienst wird erstellt, alle notwendigen Treiber werden installiert.

KinderGate wird standardmäßig unter %Program Files%\Entensys\KinderGate installiert. (nachfolgend %KinderGate%).

Bitte starten Sie Ihren Rechner nach der Installation neu.

Ersteinrichtung und Registrierung

Nachdem die Installation abgeschlossen ist, müssen Sie die ersten Filtereinstellungen festlegen und das Produkt registrieren.

Wichtig! Eine nicht-registrierte Version von KinderGate sperrt die Internetverbindung.

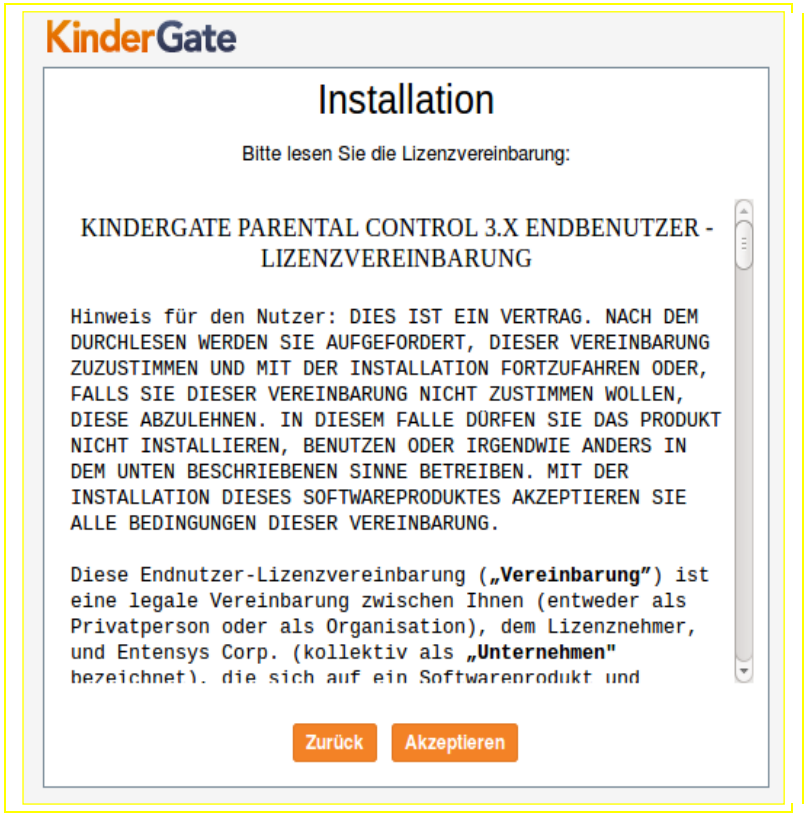
Um eine Ersteinrichtung zu beginnen, starten Sie die Verwaltungskonsole von KinderGate. Sie können dies auf mehrere Arten machen:

1. Öffnen Sie einen Webbrowser und wechseln Sie zu http://localhost:3128;
2. Versuchen Sie, eine beliebige Webseite in Ihrem Browser zu öffnen. Bis Sie das Produkt registrieren, werden Sie zu der KinderGate Verwaltungskonsole weitergeleitet;
3. Starten Sie die KinderGate Verwaltungskonsole aus der Anwendungsliste (**nur für Mac OSX**).

Nach dem ersten Start der Konsole werden Sie aufgefordert:

1. Die Sprache der Benutzeroberfläche zu wählen, z.B. Deutsch, klicken Sie danach auf Fortsetzen:

2. Lesen Sie die Lizenzvereinbarung und klicken Sie auf Akzeptieren, um die Installation der KinderGate Software fortzusetzen:


KinderGate
Installation
Bitte lesen Sie die Lizenzvereinbarung:
KINDERGATE PARENTAL CONTROL 3.X ENDBENUTZER - LIZENZVEREINBARUNG
Hinweis für den Nutzer: DIES IST EIN VERTRAG. NACH DEM DURCHLESEN WERDEN SIE AUFGEFORDERT, DIESER VEREINBARUNG ZUZUSTIMMEN UND MIT DER INSTALLATION FORTZUFAHREN ODER, FALLS SIE DIESER VEREINBARUNG NICHT ZUSTIMMEN WOLLEN, DIESE ABZULEHNEN. IN DIESEM FALLE DÜRFEN SIE DAS PRODUKT NICHT INSTALLIEREN, BENUTZEN ODER IRGENDWIE ANDERS IN DEM UNTEN BESCHRIEBENEN SINNE BETREIBEN. MIT DER INSTALLATION DIESES SOFTWAREPRODUKTES AKZEPTIEREN SIE ALLE BEDINGUNGEN DIESER VEREINBARUNG.
Diese Endnutzer-Lizenzvereinbarung („Vereinbarung") ist eine legale Vereinbarung zwischen Ihnen (entweder als Privatperson oder als Organisation), dem Lizenznehmer, und Entensys Corp. (kollektiv als „Unternehmen"
Zurück
Akzeptieren

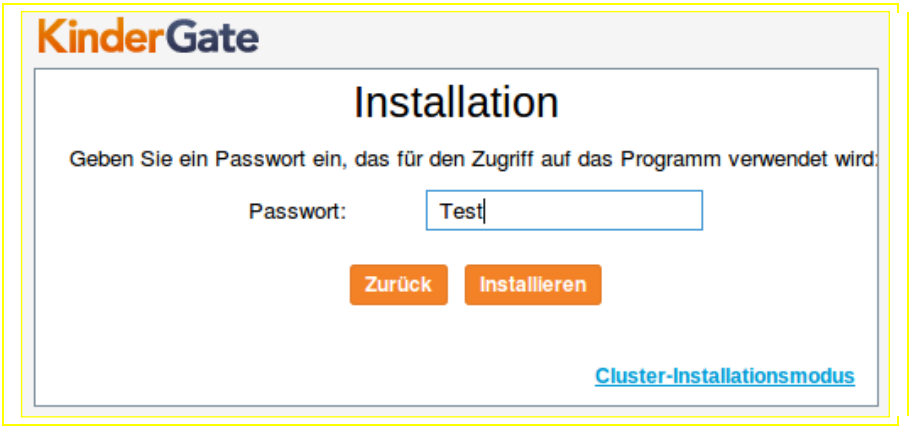
3. Wählen Sie den einfachen oder Cluster-Installationsmodus für KinderGate im Dialogfenster. Der einfache Installationsmodus ist für die Installation auf einem

einzelnen Rechner geeignet, beim Cluster-Modus werden mehrere Rechner zu einen zentralen Cluster zusammengeführt.

Einfacher Installationsmodus

Der Einfache Installationsmodus ist für die Installation auf einem einzelnen Rechner geeignet. Um ihn auszuführen, führen Sie Folgendes im Dialogfenster durch:

1. Einfachen Installationsmodus für KinderGate Software auswählen;
2. Ein Administratorpasswort für den KinderGate festlegen;
3. Installieren anklicken:



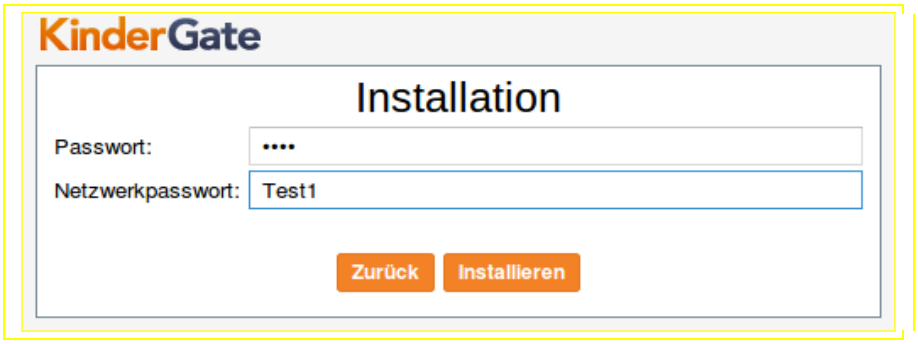
Cluster-Installationsmodus

Der Cluster-Installationsmodus für KinderGate ermöglicht Ihnen, mehrere Rechner zu einem Cluster zusammenfügen. Der Einsatz von KinderGate im Cluster erlaubt eine zentrale Anwendung von Filtereinstellungen auf allen Rechner im Cluster gleichzeitig.

Klicken Sie auf Cluster-Installationsmodus im Installationsfenster, um die Cluster-Installation für KinderGate zu wählen:

Wählen Sie den Nodetyp Masternode für die Installation von KinderGate auf dem ersten Rechner oder Slavenode für alle nachfolgenden Rechner aus.

Legen Sie das Administratorpasswort fest, falls Sie zuvor Masternode ausgewählt haben. Ein Netzwerkpasswort ist nötig, um die Rechner zum bereits existierenden Cluster hinzuzufügen. Klicken Sie auf Installieren:



Geben Sie den Namen des Masternode und das Passwort für Slavenode ein, falls Sie den Slaverechner ausgewählt haben.

Klicken Sie auf Verbinden:

Der Masternodename muss folgendermaßen aussehen: kindergate@hostname, wobei *hostname* der Name des Masternode sein muss. Der Node vom KinderGate Cluster wird auf der Lizenzseite für Administratoren angezeigt. Beim Einsatz auf Clusterebene muss die Software nur auf einem beliebigen Node registriert werden.

Wichtig! Das Administratorpasswort wird für die Verbindung zwischen Admin-Konsole und dem KinderGate-Systemdienst benötigt, sowie für die Deinstallation der Anwendung.

Lizenz für KinderGate registrieren

Um eine Lizenz für KinderGate registrieren zu können, benötigen Sie die Admin-Konsole, einen speziellen PIN-Code und einen Internetanschluss.

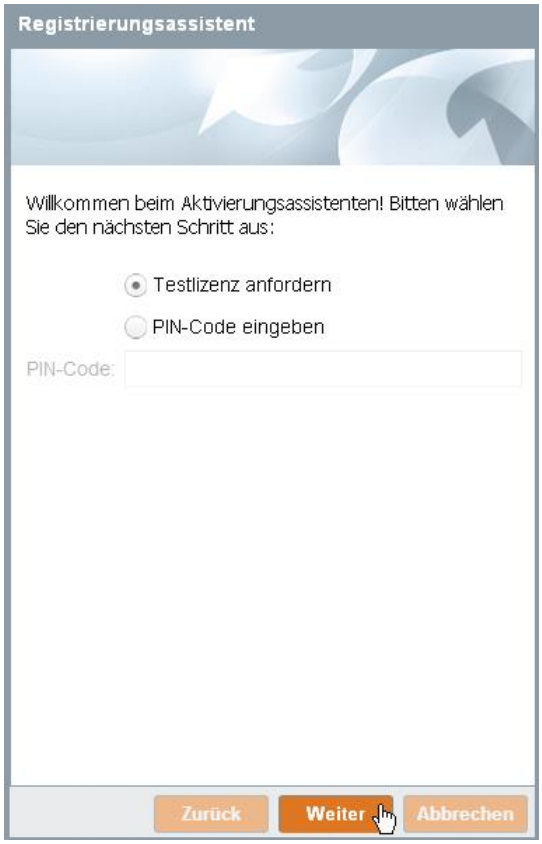
Beim Erststart der Admin-Konsole startet der Registrierungsassistent automatisch. Der Registrierungsassistent erlaubt Ihnen, einen Test- oder einen voll funktionsfähigen Schlüssel zu erwerben. Der Schlüssel sollte online mittels einer HTTPS-Anfrage auf die Webseite des Entwicklers (www.entensys.com) angefordert werden. Für die korrekte Registrierung der Lizenz ist das HTTP-Protokoll freizuschalten.

Testlizenz

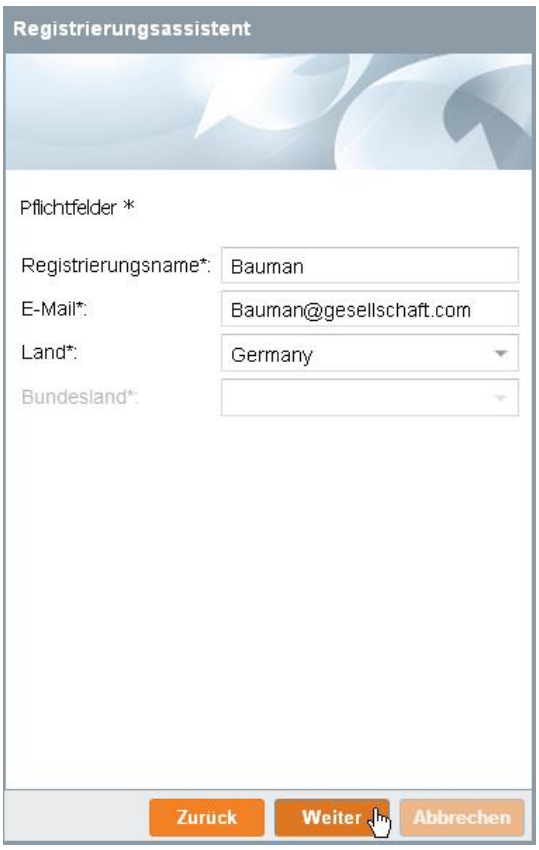
Bei der Anforderung von einem Testschlüssel wird eine 30-tägige Testlizenz generiert. Nach dem Ablauf der Testlizenz funktioniert die KinderGate Software nicht mehr, der Internetzugang wird blockiert.

Gehen Sie wie folgt im Dialogfenster des Registrierungsassistenten vor, um einen Testschlüssel zu bekommen:

- „Testlizenz anfordern“ markieren;
- „Weiter“ anklicken:



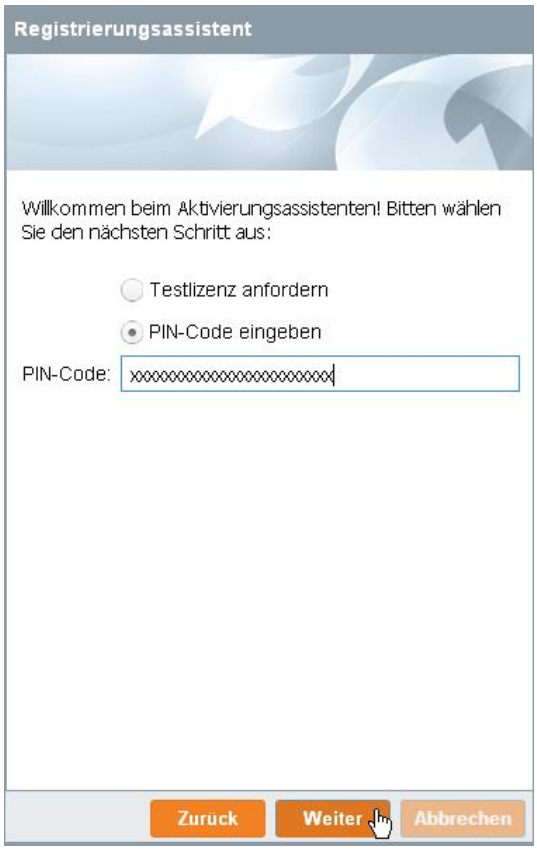
- Geben Sie einen Registrierungsnamen, E-Mail, Land und Bundesland ein, um den Installationsvorgang fortzusetzen:



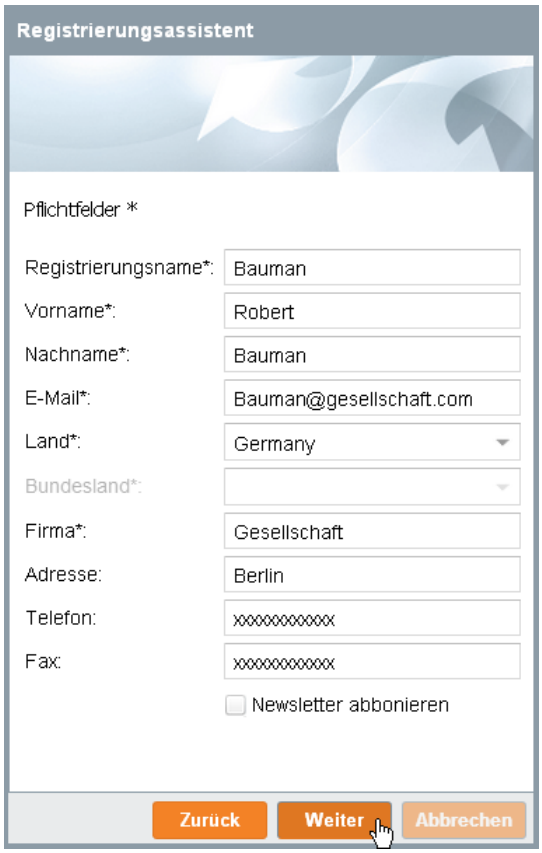
Vollwertige Lizenz

Um eine vollwertige Lizenz zu erhalten, gehen Sie im Dialogfenster des Registrierungsassistenten wie folgt vor:

- „PIN-Code eingeben“ auswählen;
- Speziellen PIN-Code, den Sie beim Erwerb der KinderGate Software bekommen haben, im Textfeld eingeben;
- „Weiter“ anklicken:



- Geben Sie einen Registrierungsnamen und persönliche Informationen ein, füllen Sie alle Pflichtfelder aus, um den Installationsvorgang fortzusetzen und teilen Sie Ihre E-Mail mit, um eine Bestätigung zu bekommen;
- Klicken Sie auf „Weiter“:



Falls Ihr Passwort verloren geht, wird eine E-Mail auf die von Ihnen während der Registrierung eingegebenen Adresse geschickt.

Updates für KinderGate

Entensys bemüht sich stets, die KinderGate Software zu verbessern. Sie werden über eine neue Version der Software benachrichtigt, indem eine neue Nachricht auf der Lizenzseite der Webkonsole erscheint.

Software Update für Linux

Sie müssen einen aktiven Internetanschluss haben, um ein Software-Update auszuführen.

Für Ubuntu und Alt Linux

Öffnen Sie die Linux-Konsole und führen Sie folgende Befehle aus:

sudo apt-get install kindergate

Software Update für Mac OSX

Laden Sie eine neue Version des KinderGate von der Seite des Entwicklers herunter und installieren Sie diese, ohne Ihre laufende Version zu deinstallieren.

Software Update für MS Windows

Laden Sie eine neue Version der KinderGate Software von der Seite des Entwicklers herunter und installieren Sie diese, ohne Ihre laufende Version zu deinstallieren. Nachdem die Installation abgeschlossen wird, starten Sie Ihren Rechner neu.

Deinstallation von KinderGate

Software-Deinstallation für Linux

Für Ubuntu und Alt Linux

Öffnen Sie die Linux-Konsole und führen Sie folgende Befehle aus:

sudo apt-get remove --purge kindergate
sudo apt-get remove --purge entensys-otp

Software-Deinstallation für MS Windows

Deinstallieren Sie die Software mithilfe der MS Windows Programmverwaltung (Systemsteuerung→Programme und Funktionen).

Software-Deinstallation für Mac OSX

Um die KinderGate Software zu deinstallieren, führen Sie die Installationsdatei aus. Das Fenster des Installationsassistenten wird geöffnet.

Wählen Sie **Uninstall.app** aus und folgen Sie den Anweisungen zur Deinstallation.

KinderGate Parental Control

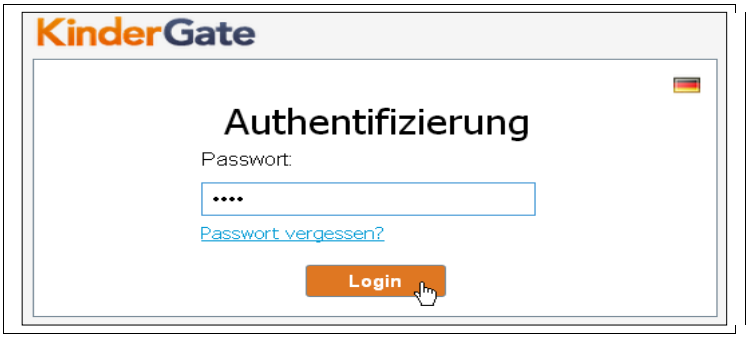
KinderGate Filtereinstellungen

Starten der KinderGate Konsole

Sie können es auf zwei Arten starten:

1. Öffnen Sie einen Webbrowser und wechseln Sie zu http://localhost:3128;
2. Sie können die KinderGate Verwaltungskonsole aus der Anwendungsliste starten (**nur für Mac OSX**).

Beim starten der KinderGate Software wird ein Authentifizierungsfenster geöffnet, in dem Sie das Administratorpasswort eingeben und auf „Login“ klicken müssen:



KinderGate Software verfügt über eine Einfache und eine Erweiterte Admin-Konsole, in welchen Sie die Filter festlegen können. Die Einfache Admin-Konsole wird beim Starten von KinderGate geöffnet.

Sie können in die erweiterte Admin-Konsole wechseln, indem Sie auf Zur erweiterten Konsole wechseln in der Kopfzeile klicken:

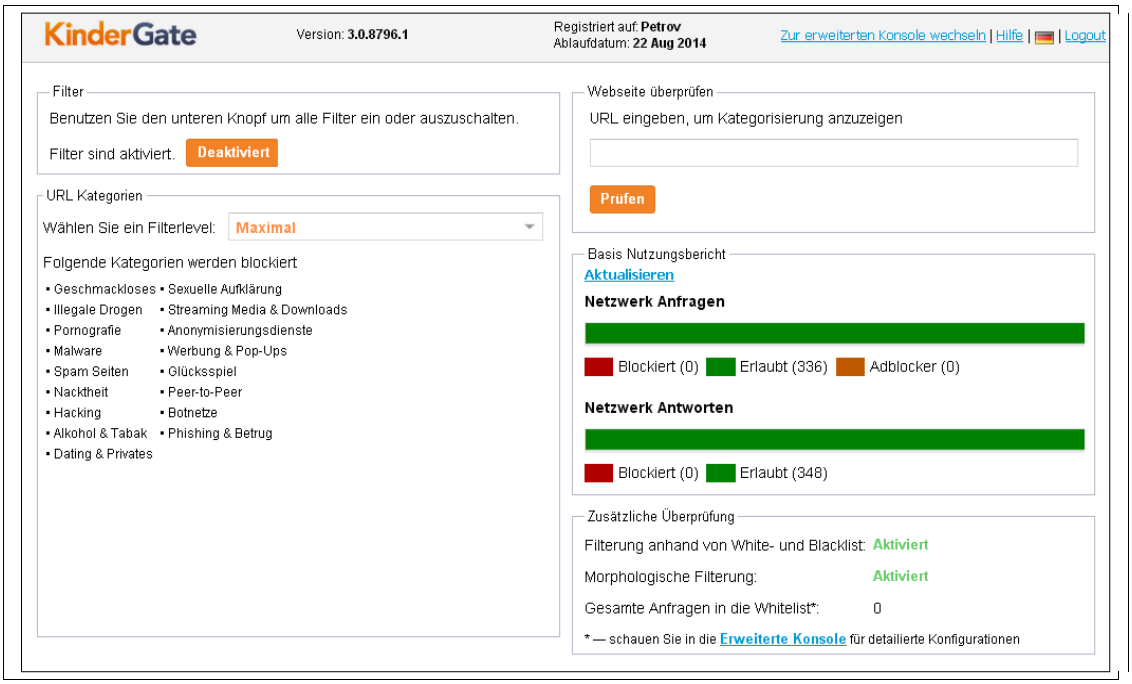
Einfache Admin-Konsole

Die einfache Admin-Konsole wird benutzt, um Filtereinstellungen anzuschauen, Filter schnell ein-/auszuschalten, Filterlevel zu wechseln, URLs zu untersuchen, Seiten zur Whitelist oder Blacklist hinzuzufügen, allgemeine Nutzungsstatistiken aufzurufen, zusätzliche Untersuchung ein-/auszuschalten oder um zur erweiterten Admin-Konsole zu wechseln.

Die Kopfzeile der einfachen Admin-Konsole auf der Webseite von KinderGate zeigt die Informationen über Softwareversion des KinderGate, Eigentümer der registrierten Lizenz und Ablaufdatum der Lizenz.

Die Einfache Admin-Konsole ist in folgende funktionale Bereiche aufgeteilt:

- Filter (Aktivieren/Deaktivieren);
- URL-Kategorien (Filterlevel auswählbar – Niedrig, Mittel, Hoch, Maximal, Alles erlauben, Benutzerdefinierte Kategorien);
- Webseite überprüfen;
- Basis Nutzungsbericht;
- Zusätzliche Überprüfung.


KinderGate
Version: 3.0.8796.1
Registriert auf: Petrov
Ablaufdatum: 22 Aug 2014
Zur erweiterten Konsole wechseln | Hilfe | | Logout
Filter
Benutzen Sie den unteren Knopf um alle Filter ein oder auszuschalten.
Filter sind aktiviert.
Deaktiviert
URL Kategorien
Wählen Sie ein Filterlevel:
Maximal
Folgende Kategorien werden blockiert
• Geschmackloses • Sexuelle Aufklärung
• Illegale Drogen • Streaming Media & Downloads
• Pornografie • Anonymisierungsdienste
• Malware • Werbung & Pop-Ups
• Spam Seiten • Glücksspiel
• Nacktheit • Peer-to-Peer
• Hacking • Botnetze
• Alkohol & Tabak • Phishing & Betrug
• Dating & Privates
Webseite überprüfen
URL eingeben, um Kategorisierung anzuzeigen
Prüfen
Basis Nutzungsbericht
Aktualisieren
Netzwerk Anfragen
Blockiert (0) Erlaubt (336) Adblocker (0)
Netzwerk Antworten
Blockiert (0) Erlaubt (348)
Zusätzliche Überprüfung
Filterung anhand von White- und Blacklist: Aktiviert
Morphologische Filterung: Aktiviert
Gesamte Anfragen in die Whitelist*: 0
* — schauen Sie in die Erweiterte Konsole für detailierte Konfigurationen

Im Bereich URL-Kategorien können Sie ein Filterlevel und Blockierung der Webseiten nach Kategorien auswählen. Das Filterlevel blockiert den Zugang zum voreingestellten Satz von Kategorien der Webseiten. Sie können den Filterlevel aus dem aufklappbaren Menü mit folgenden Einträgen auswählen:

- Alles erlauben;
- Niedrig;
- Mittel;
- Hoch;
- Maximal;
- Benutzerdefinierte Kategorien.

Der Filterlevel Alles erlauben löscht ggf. den festgelegten Satz von Kategorien und die Kategorien werden nicht blockiert. Eine bestimmte Liste der blockierten Webseite-Kategorien entspricht jedem Filterlevel. Zum Beispiel, bei einem ausgewählten Level „Niedrig“ werden folgende Kategorien blockiert:

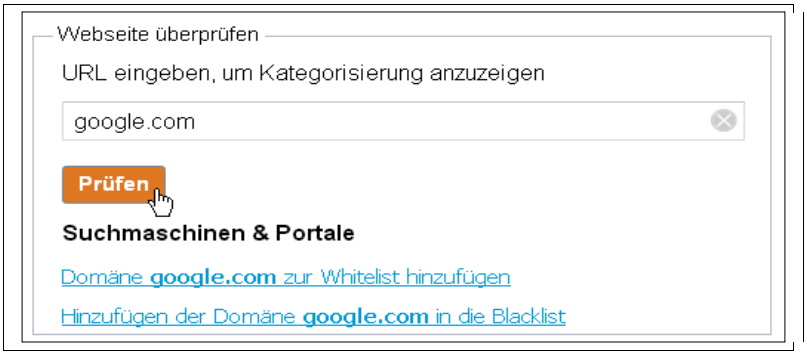
1. Werbung und Pop-ups;
2. Phishing und Betrug;
3. Malware;

4. Pornografie und Gewalt;
5. Nacktheit;
6. Botnets.

Im benutzerdefinierten Filterlevel kann der Nutzer die Kategorien individuell auswählen und blockieren.

Sie können die Kategorien im aufklappbaren Menü der URL-Kategorienliste auswählen, welche erscheint, wenn Sie auf „Wählen“ klicken. Nachdem Sie die Kategorien ausgewählt haben, klicken Sie auf die Schaltfläche „Übernehmen“.

Der Bereich „Webseite überprüfen“ wird für die schnelle Überprüfung und die Einstufung der Webseiten benutzt, sowie für das Erstellen von White- und Blacklisten. Um dies zu tun, geben Sie die Webseiten-Adresse in das Textfeld URL eingeben, um Kategorisierung anzuzeigen und klicken auf die Schaltfläche „Prüfen“. Es werden die Informationen über die Webseiten-Kategorie sowie die Vorschläge für das Hinzufügen der Webseite in die Blackliste oder in die Whiteliste angezeigt, um die Seite aus dem Ausschlussbereich zu entfernen:



Der Bereich Basis Nutzungsbericht zeigt die statistischen Daten über Internet-Nutzung, die Anzahl der Netzwerk-Anfragen und Antworten an.

Der Bereich Zusätzliche Überprüfung zeigt an, welche Filterungsmethoden neben der Filterung nach Webseiten-Kategorien aktiviert sind. Die erweiterte Admin-Konsole muss verwendet werden, um diese festzulegen.

Erweiterte Admin-Konsole

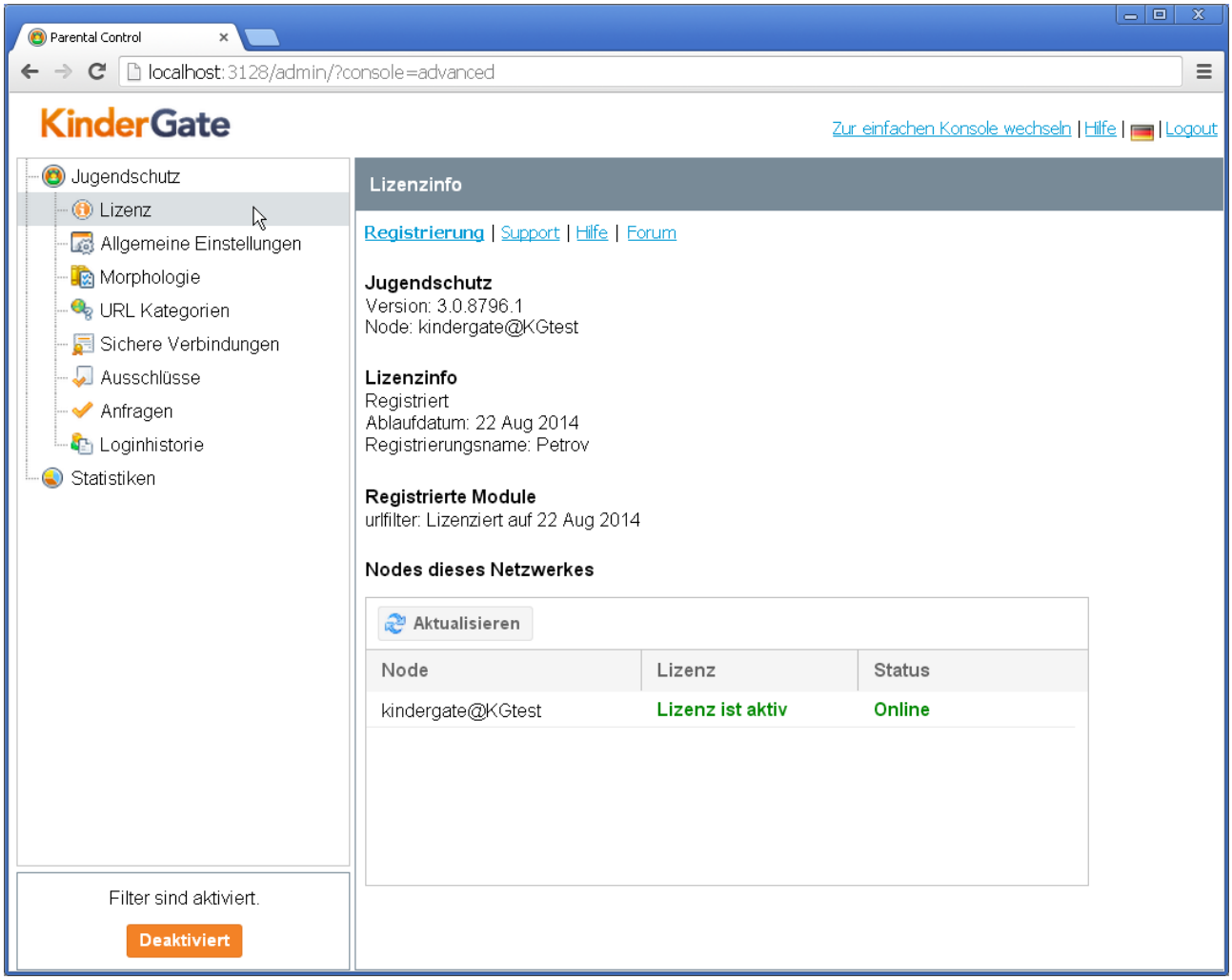
Die erweiterte Admin-Konsole kann für die Feinabstimmung des sicheren Internetzugangs oder für das Blockieren der Werbung und Banner eingesetzt werden.

Die erweiterte Admin-Konsole enthält die folgenden Bereiche:

1. Jugendschutz:
   - Lizenz;
   - Allgemeine Einstellungen;
   - Morphologie;
   - URL-Kategorien;
   - Ausschlüsse;

- Sichere Verbindungen;
- Anfragen;
- Login-Historie.

2. Statistiken;
3. Schaltfläche Filter aktivieren / deaktivieren



Die Schaltfläche „Filter aktivieren / deaktivieren“ wird verwendet, um die Filter schnell aktivieren / deaktivieren zu können und befindet sich am unteren Rand der maximierten Admin-Konsole.

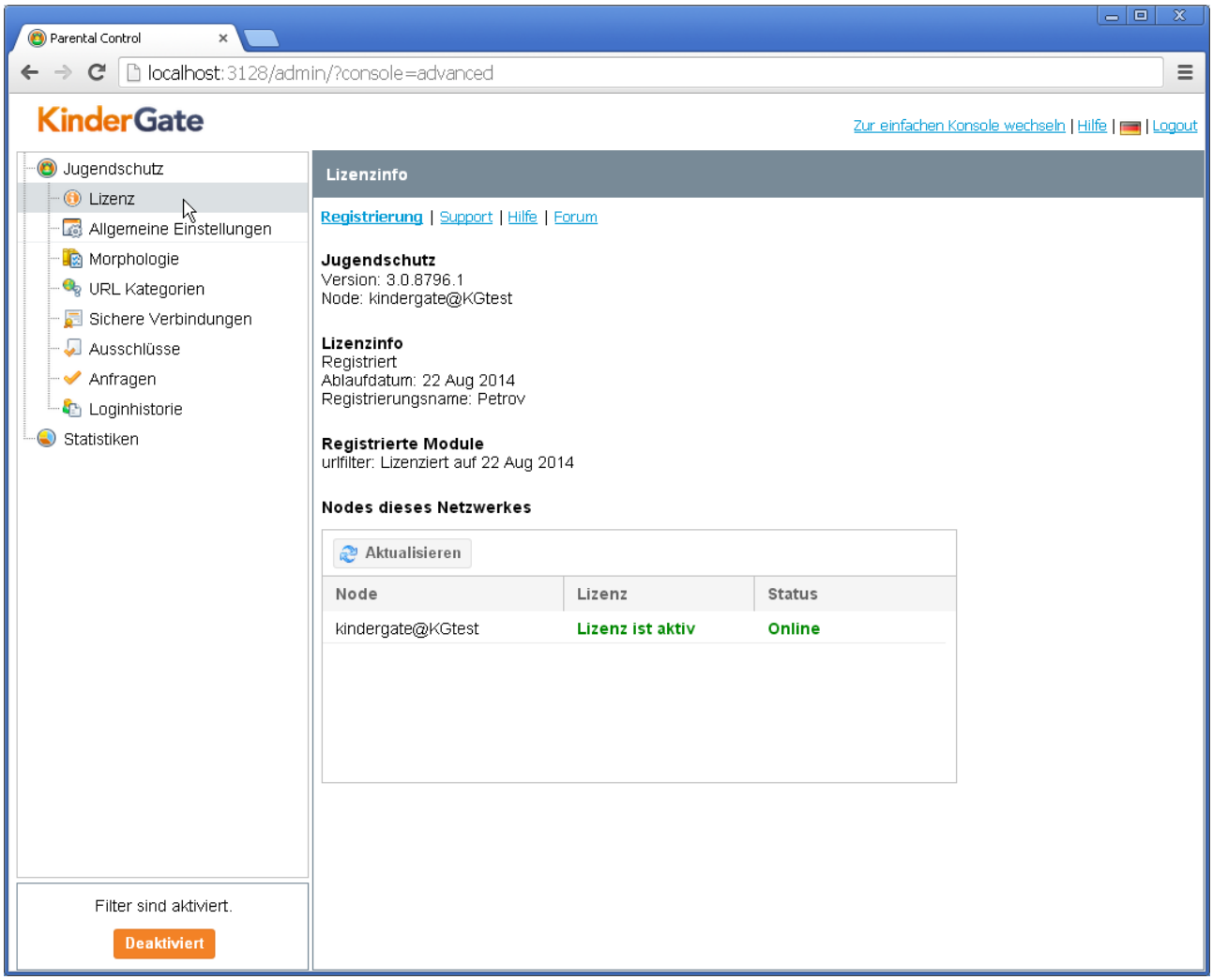
Lizenz

Der Bereich Lizenz wird verwendet, um die Lizenz zu registrieren oder um die Informationen über die Art der installierten Version von KinderGate und sein Ablaufdatum anzuschauen.

Ein Link „Neue Version ist verfügbar“ wird angezeigt, wenn eine neue Version auf der Webseite des Entwicklers zur Verfügung steht. Folgen Sie dem Link, um zu der Seite mit der neuen Version zu wechseln und Updates herunterzuladen.

Der Bereich Lizenz hat folgende Informationen:

- Version;
- Art der Version: test, registrierte, unregistrierte;
- Ablaufdatum der Lizenz;
- Registrierungsname;
- Modulname und Ablaufdatum der Registrierung;
- Informationen zu den Nodes bei einer Cluster Lizenz.



Die Lizenz-Seite hat folgende Funktionen:

- **Registrierung** – Lizenzregistrierung;
- **Support** – Link auf die Webseite des Technischen Supports;
- **Hilfe** – Link zum Online-Handbuch;
- **Forum** – Link zum Forum auf der Webseite des Herstellers, in dem die Nutzer Antworten auf ihre Fragen finden können oder mit anderen Benutzern chatten können.

Allgemeine Einstellungen

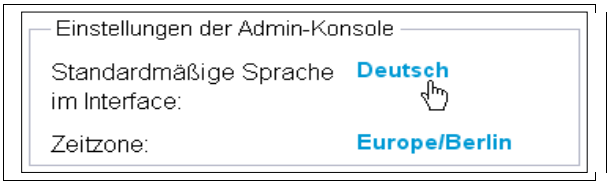
Der Bereich „Allgemeine Einstellungen“ wird verwendet, um Sprache, Zeitzone, Sichere Suche und Ad-Block festzulegen; das Herunterladen der Inhalte zu deaktivieren/ aktivieren, Zertifikate zu erstellen oder das Administratorpasswort zu ändern.

Die Seite Allgemeine Einstellungen enthält folgende Bereiche:

- Einstellungen der Admin-Konsole;
- Suche;
- Ad-block;

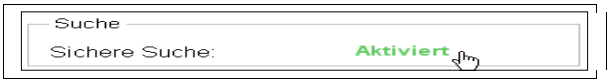
- Herunterladen von Inhalten;
- SSL-Zertifizierungsstelle;
- Passwort ändern.

Der Bereich Einstellungen der Admin-Konsole wird benutzt, um Sprache und Zeitzone festzulegen. Die Zeitzone ist für die korrekte Anzeige von Statistiken, Ereignisprotokollen und Login-Historien (in der benutzten Zeitzone) entscheidend. Die standardmäßige Sprache und Zeitzone kann aus dem aufklappbaren Menü ausgewählt werden. Das aufklappbare Menü öffnet man durch das Klicken auf die ausgewählte Sprache der Benutzeroberfläche, z.B. Deutsch, und auf die Zeitzone, z.B. Europe/Berlin:



Der Bereich Suche wird zum Aktivieren/Deaktivieren der Option Sichere Suche in Suchmaschinen wie Google, Yandex, Yahoo, Bing, Rambler, sowie YouTube usw., verwendet. Nachdem die Sichere Suche aktiviert ist, wird ein Mechanismus gestartet, der die unberechtigten Inhalte, zum Beispiel Pornografie oder Schimpfwörter, mit der Suchmaschine nicht finden lässt. Nicht nur die Webseiten werden gefiltert, sondern auch Bilder und Videos.

Sie können die Sichere Suche aktivieren / deaktivieren, indem Sie auf das Wort Aktiviert / Deaktiviert klicken:



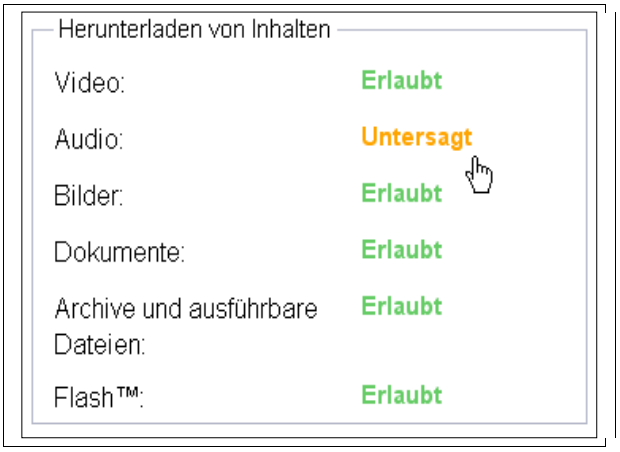
Der Bereich Ad-block wird verwendet, um Werbung und Pop-ups auf aufgerufenen Webseiten zu blockieren und um die Informationen über die laufende Version oder die neuesten Updates anzuzeigen.

Probleme mit Pop-ups verschärfen sich immer mehr. Oft hat ein Klick auf den hinter dem nervigem Bild versteckten Link nichts mit einer bewussten Entscheidung des Nutzers zu tun, sondern es ist einfach ein falscher Mausklick. KinderGate Software blockiert Pop-ups, einschließlich die von anderen Webseiten heruntergeladenen Pop-ups.

Nicht nur lästige Banner begleiten Sie, wenn Sie im Web surfen. Bei dem Besuch einer harmlosen Webseite können Ihnen auch pornografische Bilder angezeigt werden, die sich beispielsweise auf der Sidebar der Seite befinden. KinderGate Software löst auch dieses Problem, sie ist ein wahrer Zerstörer von Bannern.

Sie können Ad-block aktivieren/deaktivieren, indem Sie auf das Wort Aktiviert/Deaktiviert klicken:

Der Bereich Herunterladen von Inhalten wird verwendet, um Berechtigungen zum Herunterladen von Videos, Audio, Bildern, Dokumenten, Archiven und ausführbaren Dateien oder FLASH festzulegen. Sie müssen auf das Wort Aktiviert/Deaktiviert klicken:



Der Bereich SSL-Zertifizierungstelle ermöglicht die Einrichtung eines Zertifikats für die SSL-Verschlüsselung auf dem lokalen Rechner, dadurch werden die Browsermeldungen über SSL Zertifizierungsstellen für die gefilterte SSL-Webseiten vermieden.

Das Zertifikat muss für die korrekte Filterung des HTTPS-Datenverkehrs festgelegt sein.

Um das Zertifikat zu bekommen, klicken Sie auf auf CA-Zertifikat herunterladen im Dialogfenster für die SSL-Zertifizierungsstelle.

Das Zertifikat muss in allen auf dem Rechner verwendeten Browsern eingestellt werden. Informationen über die Einstellungen für Zertifikate in verschiedenen Browsern finden Sie im Anhang 1 dieses Handbuchs.

Der Bereich Passwort ändern ermöglicht die Änderung des alten Administratorpassworts. Um dies zu tun, geben Sie das alte und das neue Passwort ein und bestätigen Sie das neue Passwort in entsprechenden Textfeldern und klicken auf die Schaltfläche Ändern:

Morphologie

Der Bereich Morphologie wird verwendet, um Webseiten auf bestimmte Wörter und Wortkombinationen zu analysieren und enthält voreingestellte morphologische Wörterbücher.

Eine morphologische Analyse ermöglicht die Erkennung bestimmter Wörter oder Wortkombinationen auf einer Webseite, sowie die Sperrung des Zugangs zu der gesamten Webseite, falls sie unerlaubte Wörter enthält, und die Steuerung des Zugriffs auf bestimmte Bereiche einer Webseite, ohne die Blockierung der gesamten Webseite auf der Kategorie- oder Domain-Ebene.

Dieses Verfahren ist effektiv, wenn andere Verfahren den Zugang zu Webseiten oder Gruppen von Webseiten mit ähnlichem Inhalt nicht blockieren können. Eine morphologische Analyse wird verwendet, um den Zugang zu sozialen Netzwerken, Foren und anderen Webseiten, deren Inhalt meistens von Nutzern stammt, zu kontrollieren.

KinderGate überprüft den Text auf einer Webseite und berechnet seine „Gewichtung“, welche auf den „Gewichtungen“ von Worten und Wortkombinationen in den morphologischen Kategorien der Wörterbücher basiert. Wenn die „Gewichtung“ der Webseite die „Gewichtung“ der morphologischen Kategorie übersteigt, gibt KinderGate eine Meldung heraus, dass der Zugang blockiert wird.

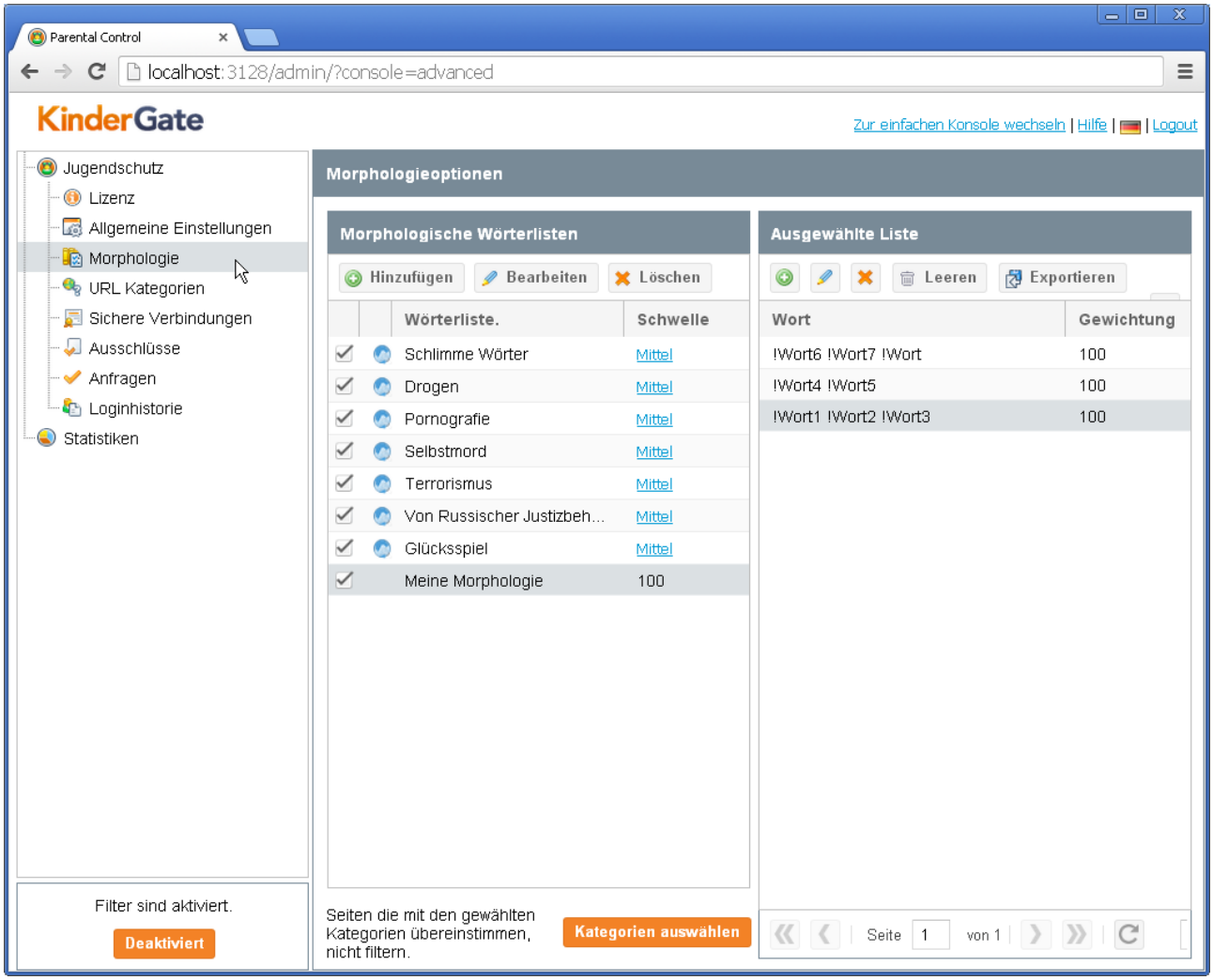
Bei der Berechnung der „Gewichtung“ einer Webseite werden alle Formen der unerlaubten Wörter berücksichtigt. KinderGate verwendet eingebaute Wörterbücher für die Sprachen Russisch, Englisch, Deutsch, Japanisch und Arabisch bei der Suche nach Wortformen.

Die KinderGate Software hat folgende standardmäßig aktivierte morphologische Wörterbücher von Entensys:

- Schlechte Worte;
- Drogen;
- Glücksspiele;
- Pornografie;
- Selbstmord;
- Terrorismus.

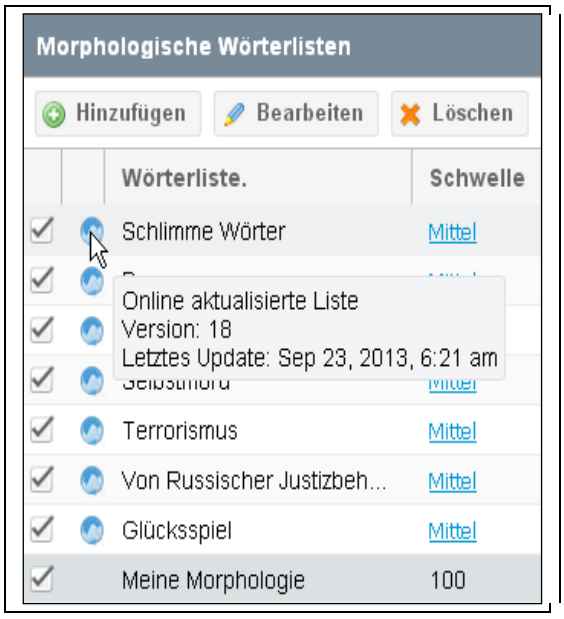
Eingebaute morphologische Wörterbücher können nicht bearbeitet oder gelöscht werden, jedoch können die Wörterbücher aktiviert/deaktiviert oder der Filterlevel geändert werden, bei der Festlegung der Regeln für die HTTP-Filterung unter Morphologieoptionen.

Morphologische Filterung wird im Bereich Morphologie auf der Seite Morphologieoptionen festgelegt:



Morphologische Wörterbücher von Entensys werden ständig aktualisiert.

Sie können die Informationen über das neueste Update der Wortlisten in einem Wörterbuch sowie die Versionsnummer ansehen, indem Sie den Mauszeiger über das Wörterbuch-Symbol bewegen:



Um ein morphologisches Wörterbuch zu deaktivieren, wählen Sie einfach das Kontrollkästchen nebenan ab. Darüber hinaus können Sie den Schwellenwert für jedes Wörterbuch ändern. Es gibt drei Filterstufen: niedrig, mittel und hoch. Sie können die Filterung für jedes morphologische Wörterbuch festlegen, indem Sie den Mauszeiger über die Stufe bewegen und sie anklicken:

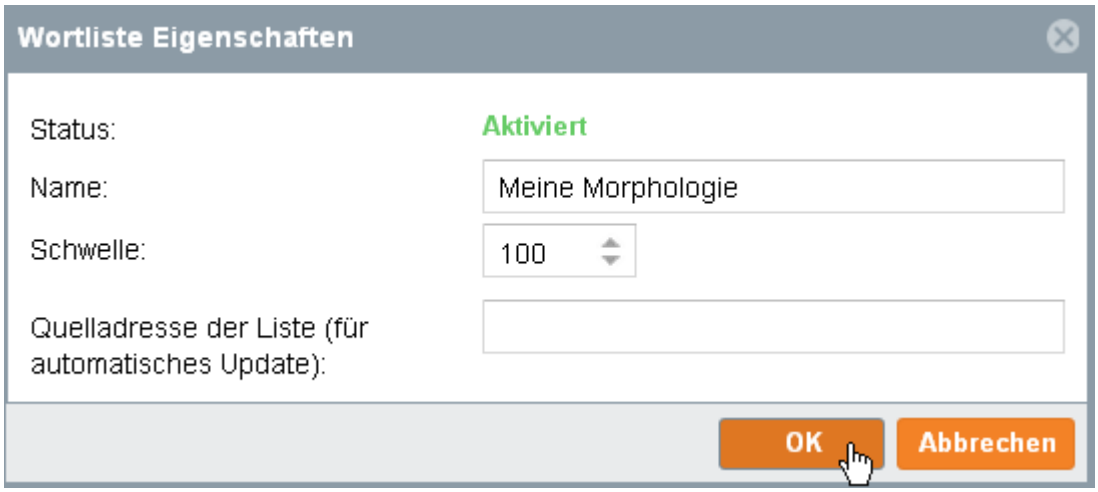
Eine morphologische Datenbank erstellen

Nutzer können ihre eigenen morphologischen Wörterbücher erstellen. Ein morphologisches Wörterbuch kann in den Bereichen Morphologische Wörterlisten auf der Seite Morphologieoptionen erstellt werden.

Um ein morphologisches Wörterbuch zu erstellen, klicken Sie auf die Schaltfläche „Hinzufügen“ im Bereich „Morphologische Wörterlisten“. Im Dialogfenster „Wortliste Eigenschaften“ gehen Sie wie folgt vor:

- Namen des Wörterbuchs eingeben;

- Wörterbuch-Status und Schwellenwert einstellen;
- Quelladresse eingeben (für automatische Updates) ;
- Schaltfläche „OK“ anklicken:



Im Bereich Ausgewählte Liste können Sie Wörter in das erstellte Wörterbuch hinzufügen, mit welchem die Webinhalte gefiltert werden.

Um ein Wort in der Liste hinzuzufügen, sollten Sie:

- Auf die Schaltfläche Hinzufügen klicken;
- Das Wort in das Textfeld eingeben;
- Die „Gewichtung“ angeben (100 standardmäßig):

Beim Hinzufügen eines Wortes ins morphologische Wörterbuch können Sie das Zeichen "!" vor dem Wort eintippen, zum Beispiel "!bassterd " . In diesem Fall wird ein Slangwort nicht in verschiedene Wortformen umgewandelt, wodurch die Wahrscheinlichkeit von falscher Blockierung reduziert wird. Sie können sowohl Wörter als auch Wortkombinationen in der Wortliste eingeben.

Falls erforderlich, dürfen Wörter in einem Wörterbuch bearbeitet oder gelöscht werden. Um dies zu tun, heben Sie das Wort hervor und klicken Sie auf Bearbeiten oder Löschen. Bearbeiten Sie das Wort direkt in der Zeile; löschen Sie das Wort, indem Sie auf Löschen klicken :

Um alle Wörter in einem Wörterbuch zu löschen, verwenden Sie die Schaltfläche „Leeren“. Sie können eine Wortliste löschen, indem Sie auf „Löschen“ klicken.

Zentrale morphologische Datenbank erstellen

Der Administrator kann persönliche Wörterbücher erstellen und sie auf alle Rechner mit installiertem KinderGate verteilen. Folgen Sie diesen Anweisungen, um eine morphologische Datenbank zu erstellen:

1. Erstellen Sie eine Datei list.txt mit einer Liste von Wörtern in folgendem Format:

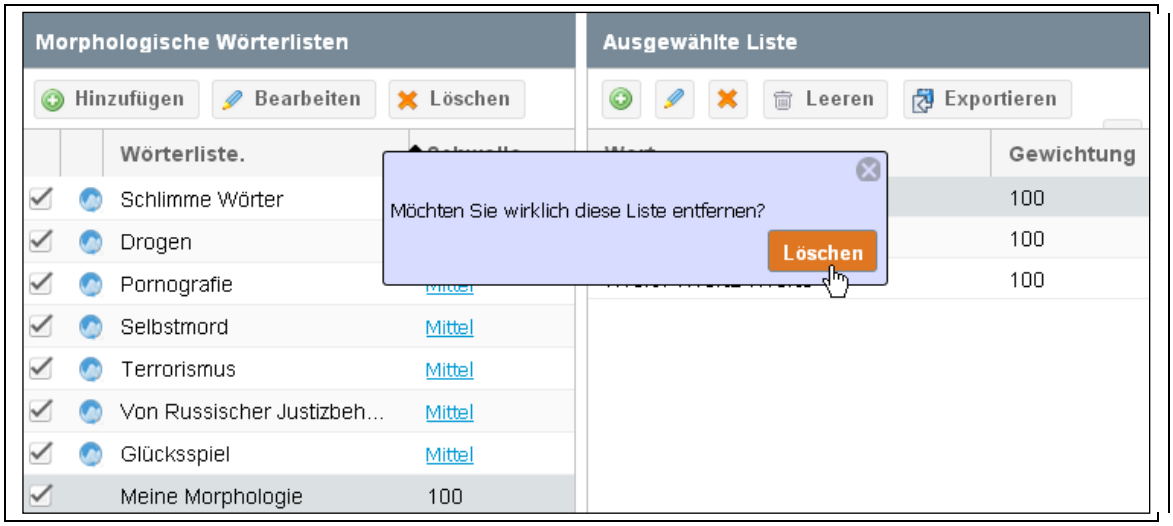
   !Wort1 !Wort2
   !Wort3
   Wort4 50
   …
   letztesWort letzteGewichtung

Hinweis: Die Gewichtung gleicht standardmäßig 100, dieser Wert kann aber geändert werden.

2. Erstellen Sie ein Archiv oder Datei mit dem Namen list.zip;
3. Erstellen Sie eine Datei version.txt und geben Sie die Versionsnummer der Datenbank in der Datei ein, zum Beispiel 2. Sie müssen diesen Wert mit jedem Update der morphologischen Datenbank entsprechend erhöhen;
4. Laden Sie die Zip-Datei und version.txt Datei auf Ihrer Webseite hoch, so dass sie zum Download zur Verfügung stehen;
5. Erstellen Sie eine morphologische Datenbank auf jedem Rechner, auf dem KinderGate installiert ist;
6. Geben Sie die Adresse für das Herunterladen der Updates an. KinderGate überprüft das Wörterbuch auf Ihrer Webseite zweimal täglich auf eine neue Version und aktualisiert es bei Bedarf.

Morphologisches Wörterbuch löschen

Sie können ein morphologisches Wörterbuch löschen, indem Sie auf die Schaltfläche „Löschen“ im Bereich Morphologische Wörterbücher klicken und dann Löschen im Dialogfenster klicken:

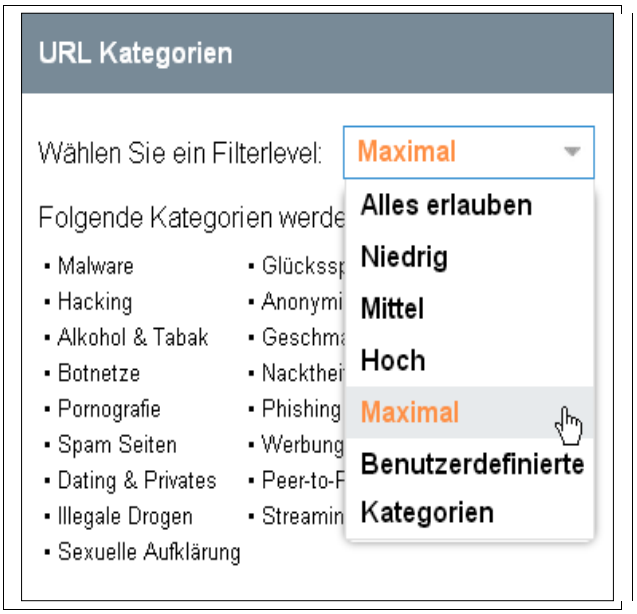


URL-Kategorien

Der Bereich URL-Kategorien wird verwendet, um die Stufe der Filterung und des Blockierens nach bestimmten Kategorien festzulegen, um Webseiten zu überprüfen oder die Filterungskategorien zu ändern und eine Änderung der Kategorie für die ausgewählte Webseite anzufordern.

Das Filterlevel verhindert automatisch den Zugriff auf voreingestellte Kategorien von Webseiten. Sie können den Filterlevel aus einem aufklappbaren Menü mit folgenden Optionen wählen:

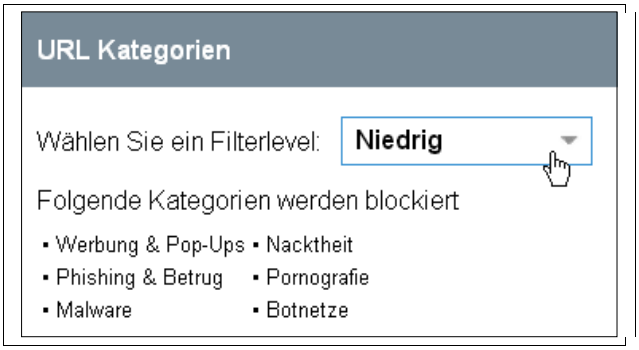
- Alles Erlauben;
- Niedrig;
- Mittel;
- Hoch;
- Maximal;
- Benutzerdefinierte Kategorien:



Das Filterlevel „Alles Erlauben“ schaltet die Filterung nach voreingestellten Kategorien aus und die Kategorien werden damit nicht blockiert:

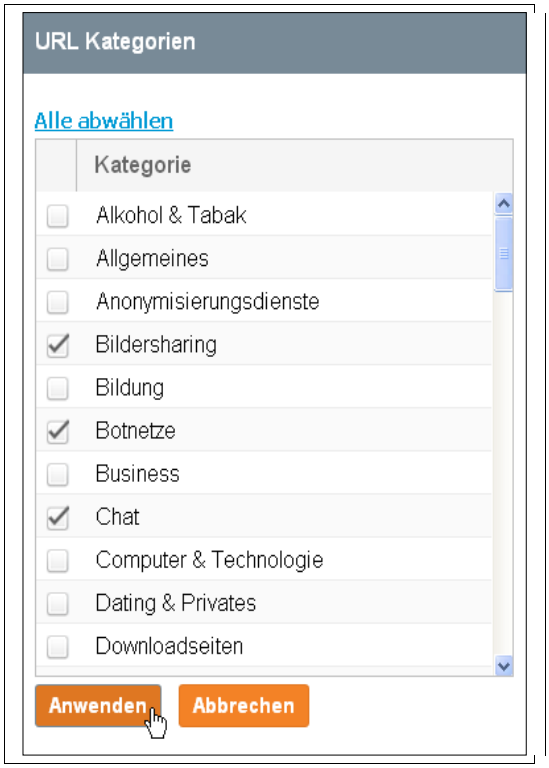
Jedem Filterlevel ist eine bestimmte Liste von blockierten Webseitenkategorien zugeordnet. Zum Beispiel, wenn das niedrige Level ausgewählt ist, werden die folgenden Kategorien gesperrt:

- Werbung & Pop-Ups;
- Phishing & Betrug;
- Malware;
- Pornografie;
- Nacktheit;
- Botnetze.



Das Filterlevel „Benutzerdefinierte Kategorien“ lässt dem Benutzer alle für ihn relevanten Kategorien auswählen und blockieren:

Die Auswahl der Kategorien erfolgt im aufklappbaren Menü unter URL-Kategorien, welches sich beim Klick auf „Auswählen“ öffnet. Nachdem Sie die Kategorien ausgewählt haben, klicken Sie auf die Schaltfläche „Anwenden“:

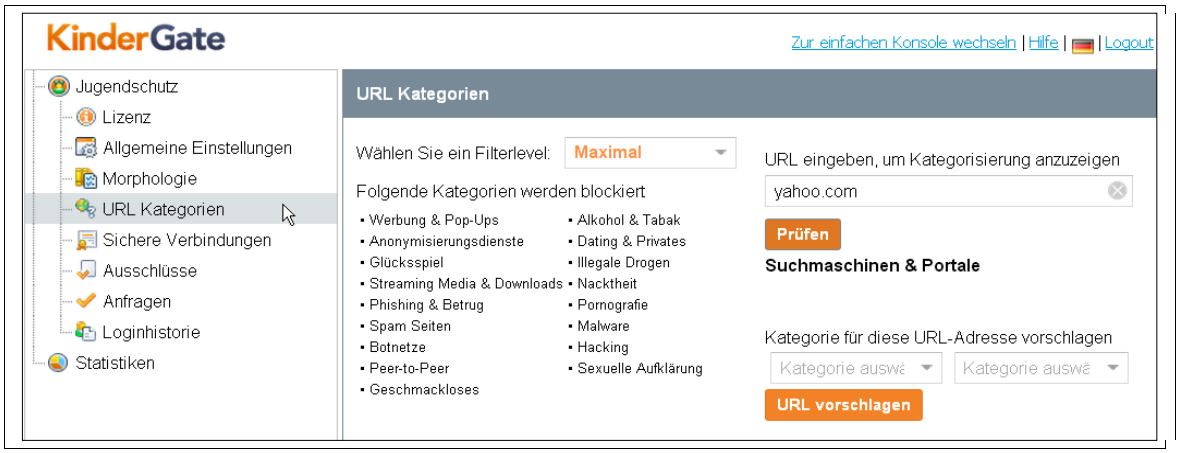


Das Textfeld „URL-Adresse eingeben, um die Einordnung anzuzeigen“ wird verwendet, um die Kategorie einer Webseite zu überprüfen, eine Neuzuordnung zu einer anderen Kategorie anzufordern, falls die laufende Kategorie mit dem Webseiteninhalten nicht übereinstimmt und um zu überprüfen, welche morphologische Datenbank die eingegebene Adresse blockiert (bei Verwendung eines morphologischen Filters).

Gehen Sie wie folgt vor, um die Kategorisierung anzuschauen:

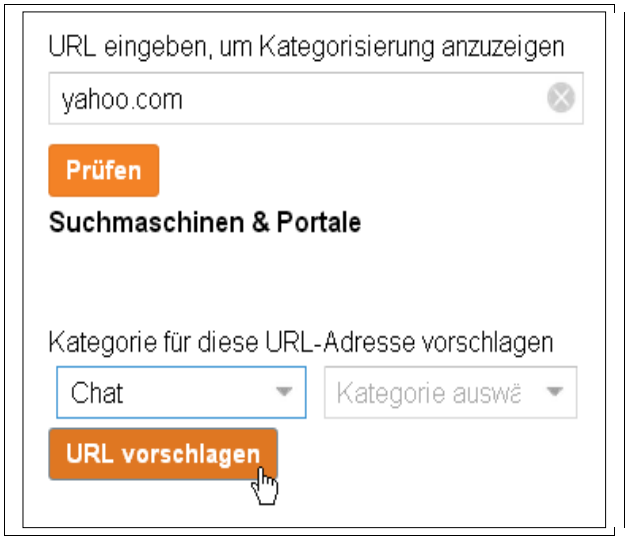
- Geben Sie die URL-Adresse ein;
- Klicken Sie auf die Schaltfläche „Prüfen“.

Wenn die Webseite bereits zu einer überwachten Kategorie auf der Seite Sichere Verbindung zugeordnet ist, zum Beispiel der Kategorie Glücksspiele, können Sie den Namen dieser Kategorie erfahren, nachdem Sie auf die Schaltfläche „Prüfen“ klicken:

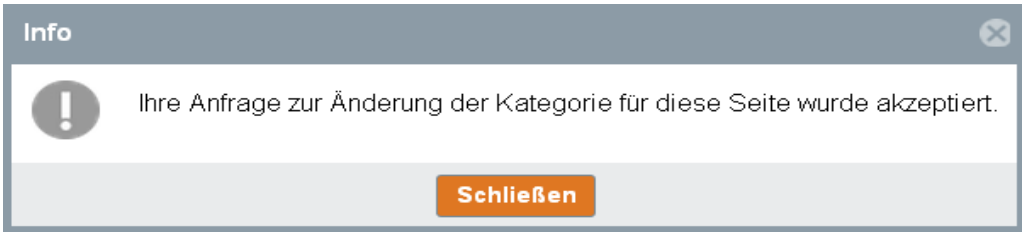


Wenn Sie glauben, dass die Kategorie der Webseite nicht zu deren Inhalt passt, können Sie einen Antrag auf Änderung der Kategorie an Entensys wie folgt abschicken:

- Wählen Sie die Kategorie der vorgeschlagenen Kategorie für diese URL im aufklappbarem Menü aus;
- Klicken Sie auf die Schaltfläche „URL vorschlagen“:



Nachdem Sie eine Anfrage zur Änderung der Kategorie abgeschickt haben, bekommen Sie folgende Meldung angezeigt: „Ihre Anfrage zur Änderung der Kategorie für diese Seite wurde akzeptiert.“:

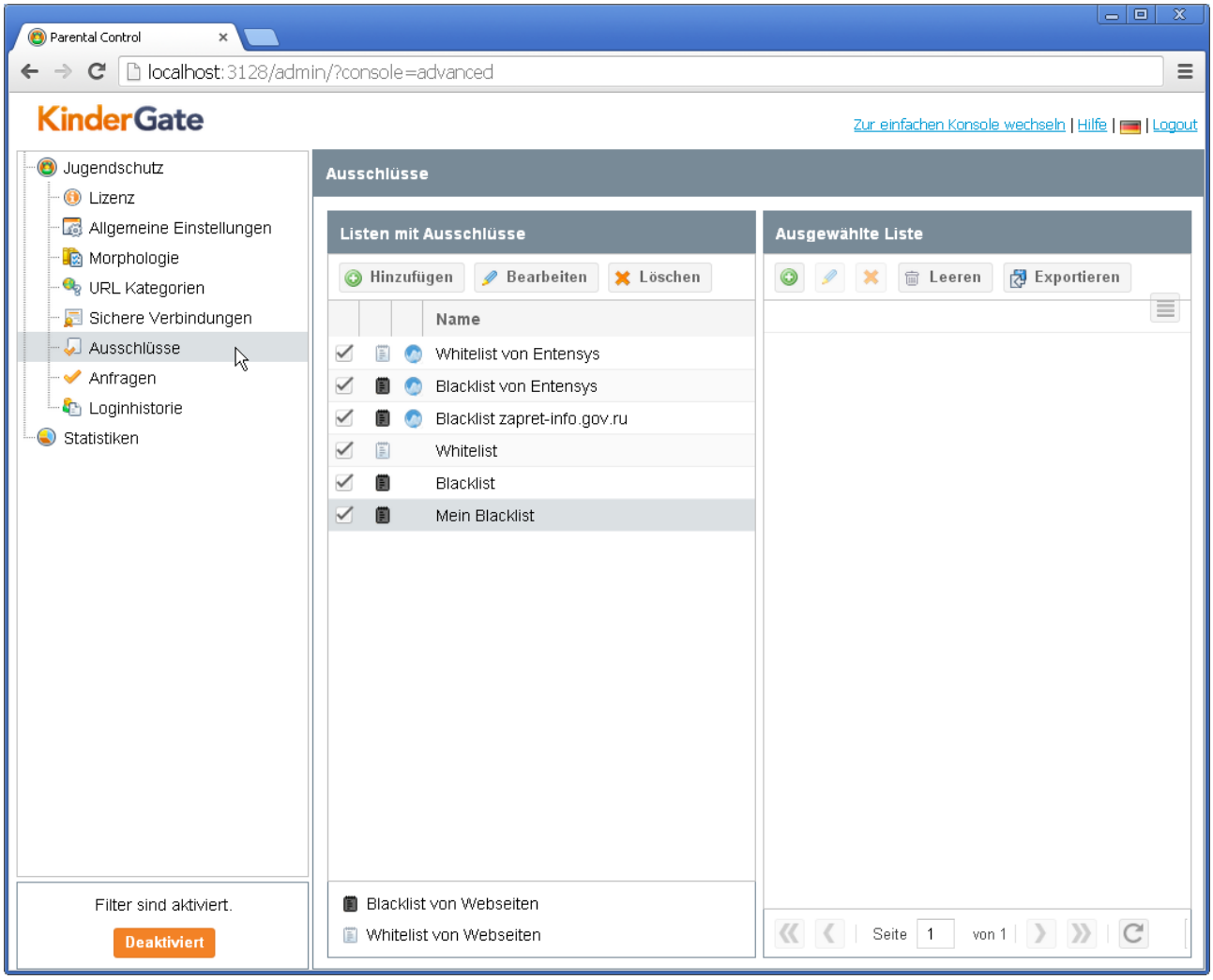


Ausschlüsse

Der Bereich Ausschlüsse dient zum Erstellen und Aufrechterhalten von Whitelisten und Blacklisten der Webseiten.

Der Bereich Ausschlüsse enthält voreingestellte standardmäßige White -und Blacklisten, die von Entensys automatisch aktualisiert werden.

Blacklisten sind die Listen der Webseiten, die immer blockiert werden. Whitelisten enthalten die Webseiten, welche immer erlaubt werden. Wenn sich dieselbe Webseite (URL) gleichzeitig in einer Whiteliste und Blackliste befindet, hat die Blackliste Priorität. Die Webseite wird also blockiert.



Sie können Platzhalter in den Listen verwenden:

- * – Beliebige Anzahl beliebiger Symbole;
- ? – Ein beliebiges Symbol.

Die Formatierung für die Liste ist in der Tabelle dargestellt:

Beispiel des Eintrags	Aktion
yahoo.com	Die gesamte Domain und alle URLs dieser Domäne werden blockiert, Domäne der 3. Ebene werden nicht blockiert.
yahoo.com*	Die gesamte Domäne und alle URLs dieser Domäne werden blockiert, Domäne der 3. Ebene werden nicht blockiert.
.yahoo.com	http://any.yahoo.com/any/ ist blockiert
yahoo.com/12345/qwer	Nur yahoo.com/12345/qwer ist blockiert
yahoo.com/12345/*	yahoo.com/12345/ jede/

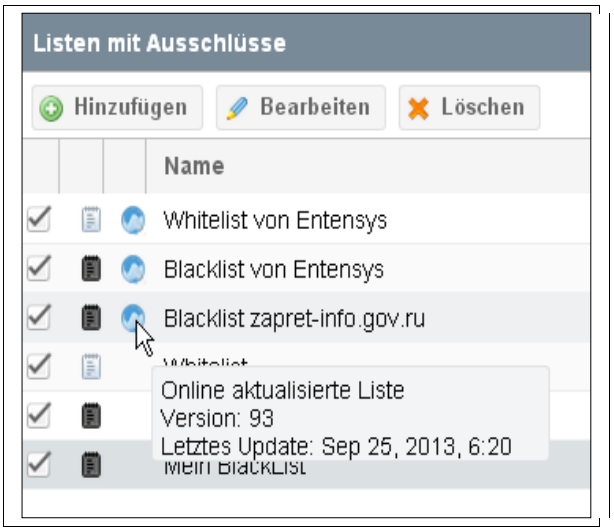
Benutzer können ihre eigenen Black- oder Whitelisten erstellen. Darüber hinaus hat in großen Einrichtungen der Administrator die Möglichkeit, Listen zu erstellen und sie zentralisiert auf allen Rechnern, auf denen KinderGate installiert ist, zu verteilen. Gehen Sie wie folgt vor, um eine Liste zu erstellen:

1. Erstellen Sie eine Textdatei mit folgendem Format:

   www.seite1.com/url1
   www.seite2.com/url2
   …
   www.seiteende.com/urlN

2. Erstellen Sie ein Archiv mit dem Namen list.zip;
3. Erstellen Sie eine Datei version.txt und geben Sie die Versionsnummer der Datenbank in der Datei ein, zum Beispiel 2. Sie müssen diesen Wert mit jedem Update der morphologischen Datenbank entsprechend erhöhen;
4. Laden Sie die Zip-Datei und version.txt-Datei auf Ihrer Webseite hoch, sodass sie zum Download zur Verfügung stehen, zum Beispiel unter folgenden Adressen: http://companyweb.com/filtering/list1/list.zip; http://companyweb.com/filtering/list1/version.txt.
5. Erstellen Sie eine zu aktualisierende Liste auf jedem Rechner mit KinderGate und geben Sie die Adresse zum Herunterladen ein. KinderGate überprüft die Versions-Datei auf Ihrer Webseite zweimal täglich auf eine neue Version und aktualisiert sie bei Bedarf.

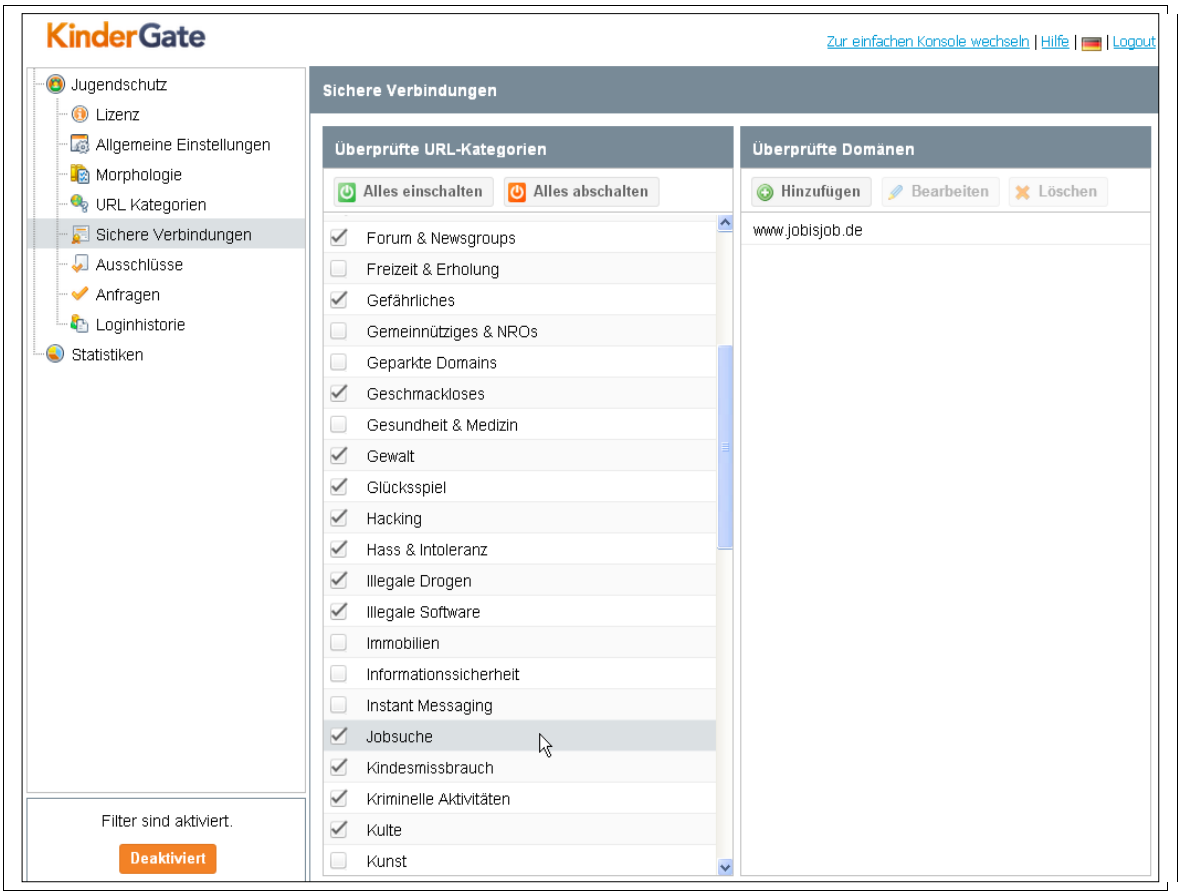
Sie können die Informationen über die neuesten Updates für die Liste sowie die Versionsnummer anschauen, indem Sie den Mauszeiger über das Webseitensymbol bewegen:



Sichere Verbindung

Die sichere Verbindung wird verwendet, um eine Filterung der HTTPS-Inhalte einzurichten. Es wird das Prinzip Man-In-The-Middle benutzt, die eine Entschlüsselung der Inhalte ermöglicht. Die Entschlüsselung wird für auf dieser Seite angegebene Webseiten oder Webseiten-Kategorien durchgeführt. Nach der Entschlüsselung wird die Filterung nach festgelegten Regeln (Morphologie, Whitelist, Blacklist, Webseiten-Kategorien, etc.) getätigt.

- **Der Bereich Überprüfte URL Kategorien** ermöglicht die Festlegung der Webseiten-Kategorien, für welche die HTTPS-Entschlüsselung durchgeführt wird;
- **Der Bereich Überprüfte Domäne** ermöglicht die Festlegung einer Liste von Webseiten, für welche die HTTPS-Entschlüsselung durchgeführt wird. Sie können die Platzhalter „*“ und „?“ . bei der Eingabe von Webseiten benutzen – zum Beispiel, *facebook.com:



Wichtig! Bei der Verwendung der HTTPS-Filterung kann der Benutzer möglicherweise eine Fehlermeldung bezüglich des Server-Zertifikats erhalten. Um solche Nachrichten zu vermeiden, laden Sie das Authentifizierungszertifikat auf Ihren Rechner herunter und richten Sie es ein. Weitere Details finden Sie im Anhang 1 zu diesem Handbuch.

Für die HTTPS-Filterung gehen Sie wie folgt vor:

- Wählen Sie Kategorien oder URLs von Webseiten, die gefiltert werden müssen. Um alle Webseiten zu filtern, geben Sie „*“ in die URL-Liste ein;
- Laden Sie das SSL-Zertifikat herunter und richten Sie es im Bereich „Allgemeine Einstellungen“ ein.

Anfragen

Der Bereich Anfragen wird verwendet, um harmlose Webseiten der Whitelist hinzuzufügen und die Informationen über Benutzeranfragen für die Verschiebung der Webseiten zu der Whitelist anzuzeigen.

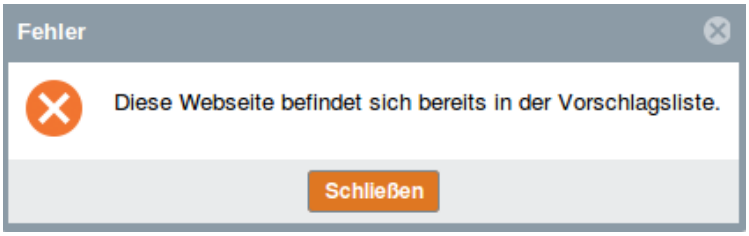
Benutzeranfragen werden auf der Seite Anfragen angezeigt und ermöglichen es dem Administrator:

- Die Webseite zu besuchen, um ihren Inhalt anzuschauen;
- Die vom Benutzer angeforderte URL zur Whitelist hinzuzufügen, falls die Seite harmlos ist;

- Die Anfrage für die Whitelist zu löschen, wenn die angeforderte Webseite unzulässig oder gefährlich ist;
- Die auf der Seite angezeigte Informationen zu aktualisieren;
- Den Node(-rechner) erkennen, von welchem die Anfrage gesendet wurde:

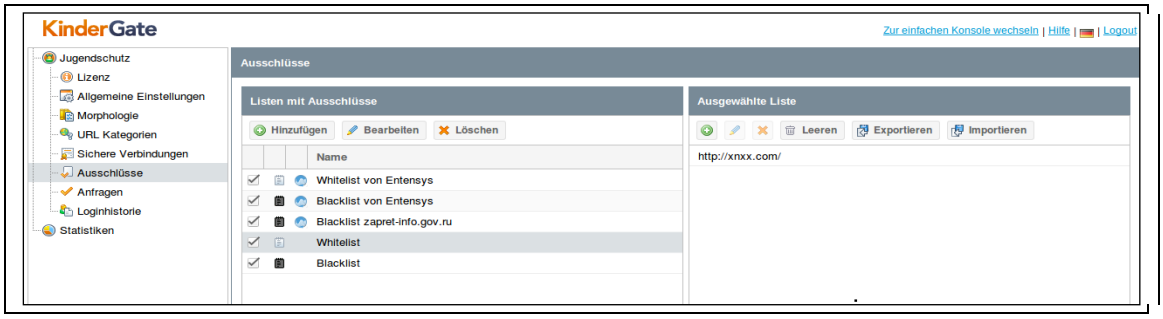
Bei einem Versuch auf eine gesperrte URL zuzugreifen, wird dem Benutzer die Meldung „Blockiert“ angezeigt, die Informationen über die blockierte Webseite (URL, Kategorie, Grund) enthält, und einen Vorschlag, die Seite zur Whitelist hinzuzufügen oder zu entsperren.

Wenn der Benutzer eine solche Meldung bekommt, kann er eine Anfrage zum Entsperren der Webseite an den Administrator schicken, indem er auf „Anfrage zum Hinzufügen in die Whitelist“ anklickt.



Die blockierte URL wird auf der Anfragen-Seite der Admin-Konsole angezeigt. Die Benutzeranfrage zum Entsperren der Webseite muss vom Administrator analysiert werden. Wenn die Webseite harmlos ist, kann sich der Administrator dafür entscheiden, die Webseite zur Whitelist hinzuzufügen, indem er auf die Schaltfläche „Zur Whitelist hinzufügen“ anklickt:

Die URL der angefragten Seite wird in den Bereich Ausschlüsse verschoben, unter Liste der Ausschlüsse, Whitelist:

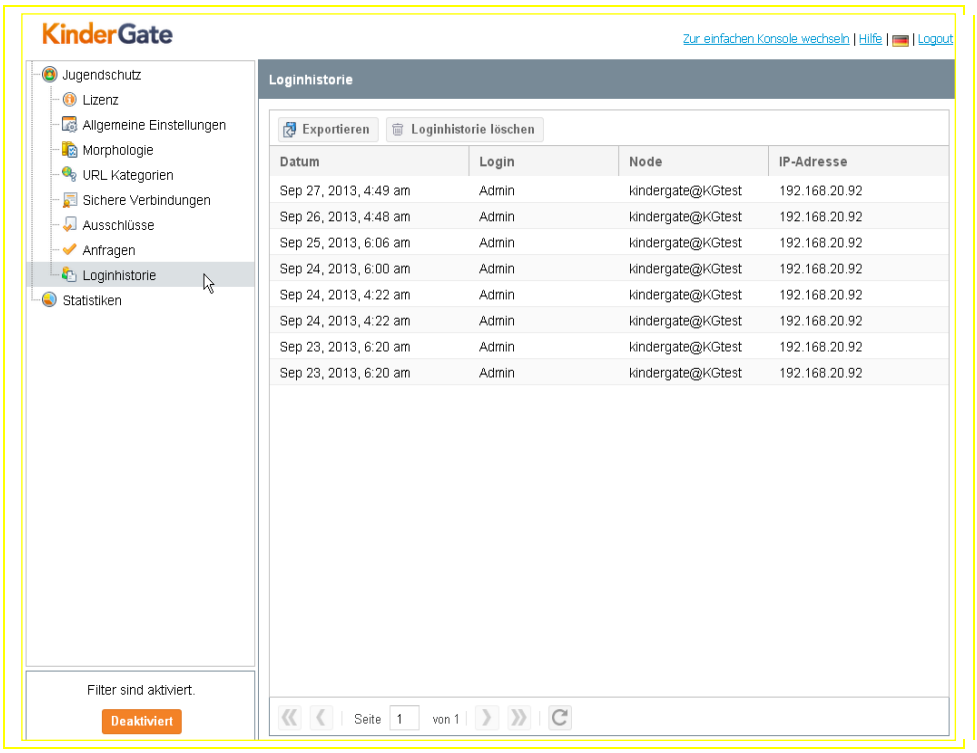


Login-Historie

Die Login-Historie wird verwendet, um den Verlauf zu Einstellungen und Aktionen des Systemadministrators, Authentifizierungen auf einem bestimmten Rechnernode oder eine Gruppe von Rechnern, die in einem Cluster gebunden sind, zu dokumentieren.

Die Seite Login-Historie enthält Informationen über das Datum der Anmeldung, Benutzernamen, Benutzernode, erste IP-Adresse und hat folgende Funktionen:

- Export - um die Login-Historie auf die lokale Festplatte als Textdatei zu exportieren;
- Die komplette Liste leeren:



Die Seite Login-Historie hat eine Navigationszeile am unteren Rand. Die Navigationszeile wird verwendet, um die Seiten durchzublättern und die Login-Historie zu aktualisieren:

Statistiken

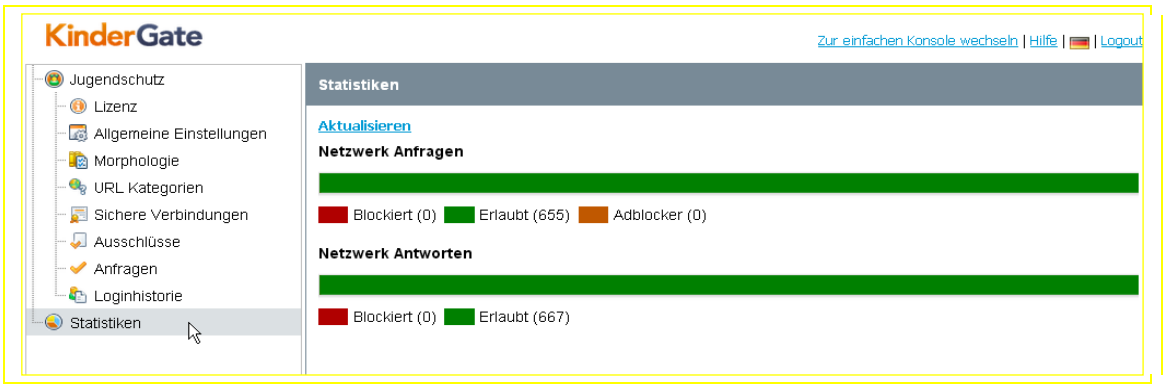
Die Seite Statistiken wird verwendet, um Daten zur Internetnutzung zu sammeln, anzuzeigen und zu aktualisieren. Die Daten werden nach der Anzahl der Netzwerkanfragen und Antworten auf die Netzwerkanfragen sortiert.

Informationen über die Anzahl und Art der ausgehenden Netzwerkanfragen haben den folgenden Status:

- Blockiert;
- Erlaubt;
- Adblocker.

Informationen über die Anzahl und Art der Netzwerkantworten haben den folgenden Status:

- Blockiert;
- Erlaubt.


KinderGate
Zur einfachen Konsole wechseln | Hilfe | | Logout
Jugendschutz
Lizenz
Allgemeine Einstellungen
Morphologie
URL Kategorien
Sichere Verbindungen
Ausschlüsse
Anfragen
Loginhistorie
Statistiken
Statistiken
Aktualisieren
Netzwerk Anfragen
Blockiert (0) Erlaubt (655) Adblocker (0)
Netzwerk Antworten
Blockiert (0) Erlaubt (667)

KinderGate Parental Control

Technischer Support

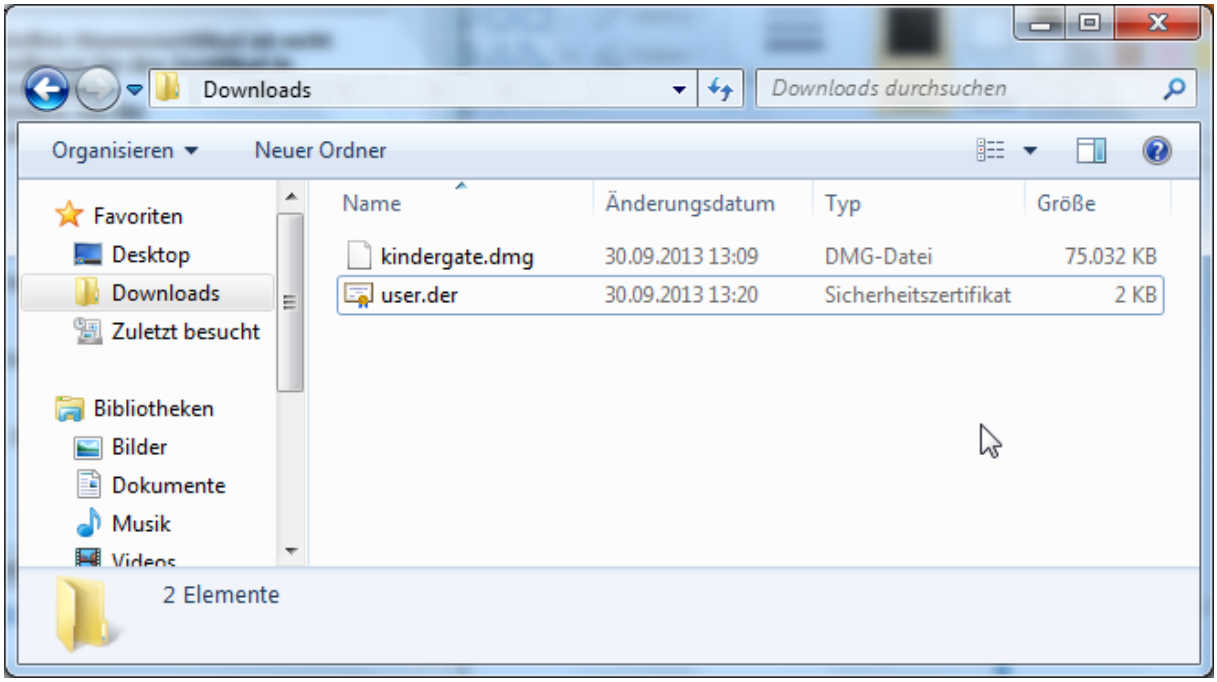
Den technischen Support finden Sie unter http://www.support.entensys.de. Dort befinden sich weitere Informationen zum Einrichten des KinderGate. Zusätzlich können Sie eine Supportanfrage zu einem Problem absenden oder die Antwort auf Ihre Frage in unserer Knowledge Base finden.

Anhänge

Anhang 1. Einrichtung eines lokalen Zertifizierungsstellen-Stammzertifikats

Einrichtung des Zertifikats für Internet Explorer und Chrome unter MS Windows

Öffnen Sie den Ordner, in dem Sie das Zertifikat gespeichert haben und klicken Sie doppelt auf das Zertifikat (user.der):

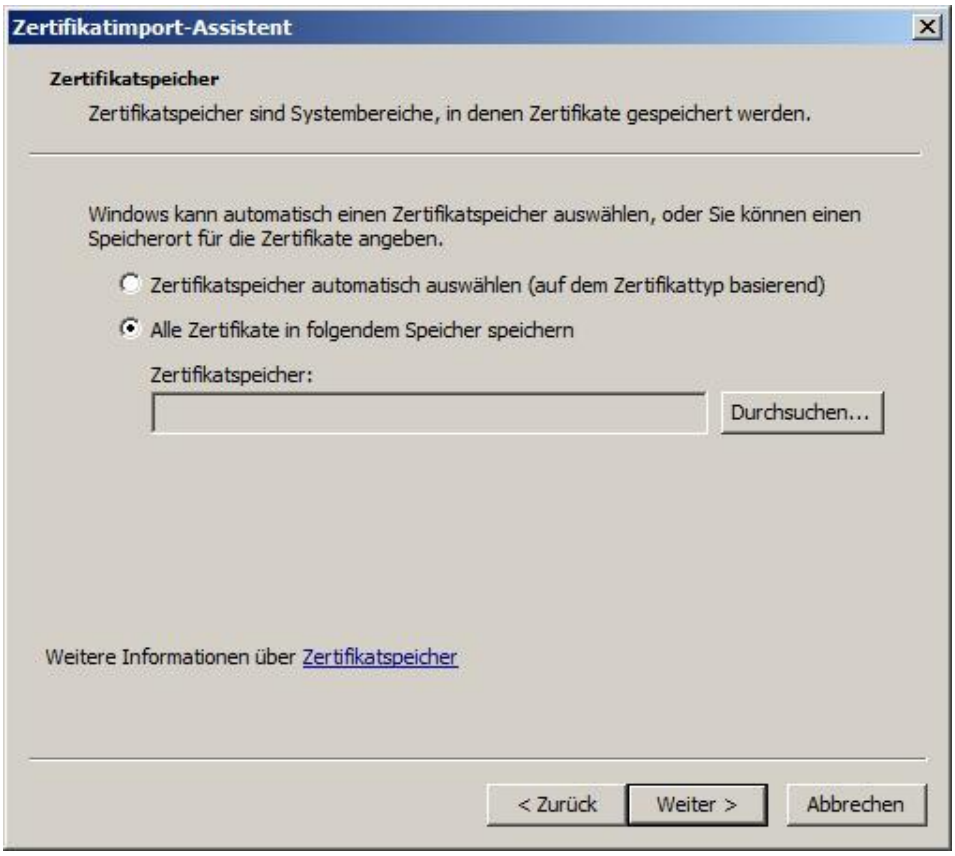


Ein Fenster mit Informationen zum Zertifikat wird geöffnet. Klicken Sie auf die Schaltfläche „Zertifikat installieren“:

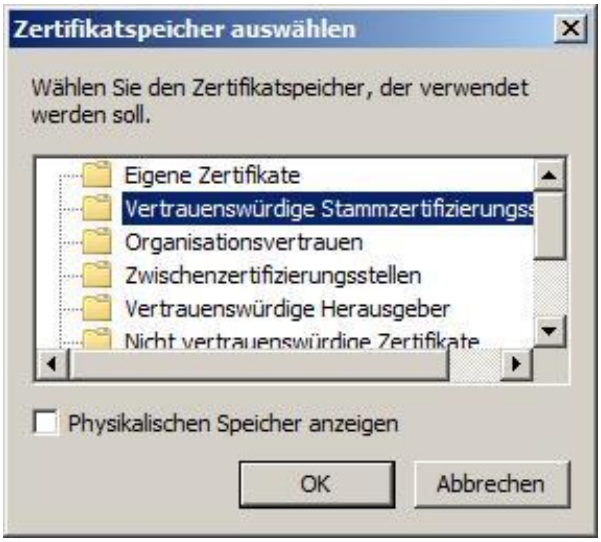
Ein Zertifikat-Importassistent wird gestartet. Führen Sie den Import durch, indem Sie allen Anweisungen des Zertifikat-Importassistenten folgen:

Zertifikatimport-Assistent
Willkommen
Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und -sperrlisten vom Datenträger in den Zertifikatspeicher.
Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
< Zurück
Weiter >
Abbrechen

Wählen Sie „Alle Zertifikate“ in folgendem Speicher speichern aus und klicken Sie auf „Durchsuchen“:

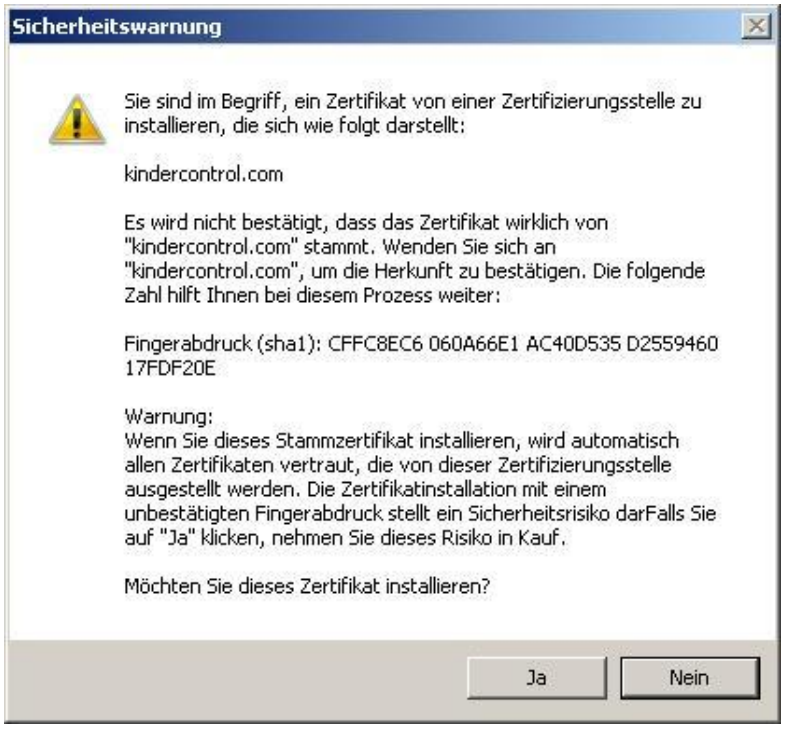

Zertifikatimport-Assistent
Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.
Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
Alle Zertifikate in folgendem Speicher speichern
Zertifikatspeicher:
Durchsuchen...
Weitere Informationen über Zertifikatspeicher
< Zurück
Weiter >
Abbrechen

Wählen Sie „Vertrauenswürdige Stammzertifizierungstellen“ aus und klicken Sie auf „OK“:



Dann klicken Sie auf „Weiter“ und „Fertig stellen“:

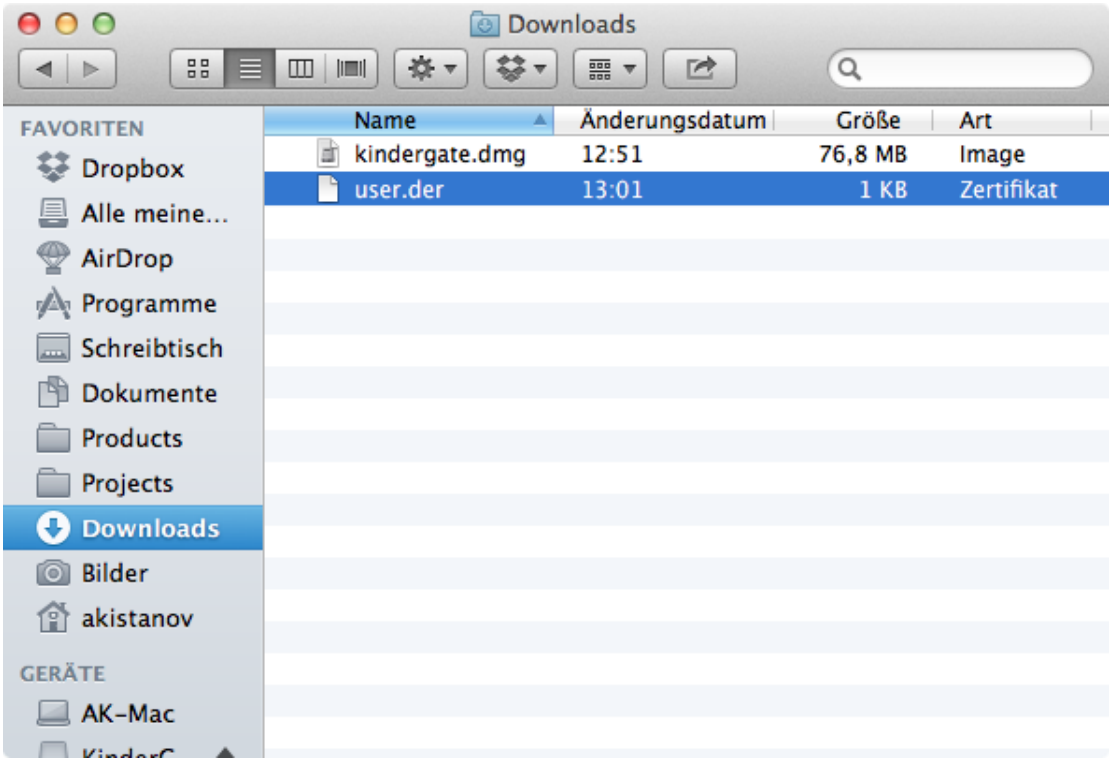
Falls eine Sicherheitswarnung erscheint, klicken Sie auf „Ja“:


Sicherheitswarnung
Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:
kindercontrol.com
Es wird nicht bestätigt, dass das Zertifikat wirklich von "kindercontrol.com" stammt. Wenden Sie sich an "kindercontrol.com", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:
Fingerabdruck (sha1): CFFC8EC6 060A66E1 AC40D535 D2559460 17FDF20E
Warnung:
Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Zertifikatinstallation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko darFalls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.
Möchten Sie dieses Zertifikat installieren?
Ja
Nein

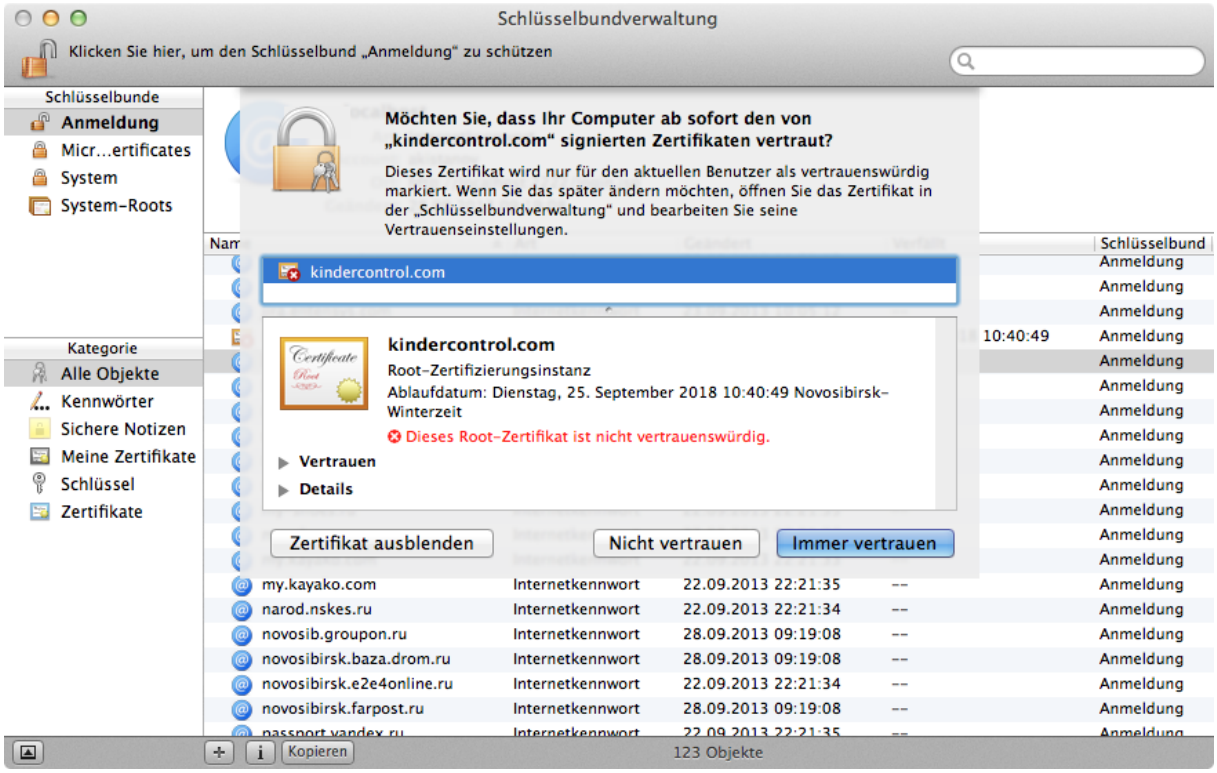
Die Einrichtung des Zertifikats ist nun abgeschlossen.

Einrichtung des Zertifikats für Safari und Chrome unter Mac OSX

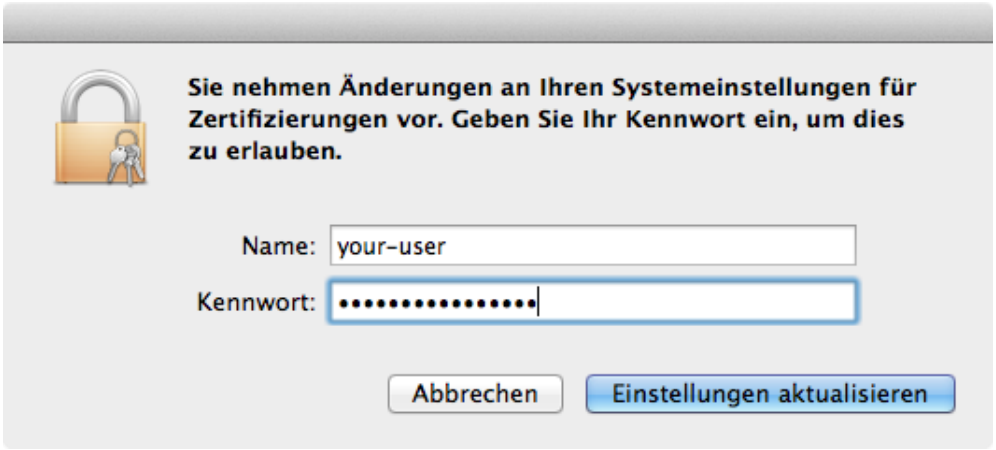
Öffnen Sie den Ordner, in dem Sie das Zertifikat gespeichert haben und klicken Sie doppelt auf das Zertifikat:



Die Schlüsselbundverwaltung wird gestartet. Wählen Sie bei diesem Zertifikat **„Immer vertrauen“**:



Geben Sie Ihr Passwort ein, um den Vorgang zu bestätigen:

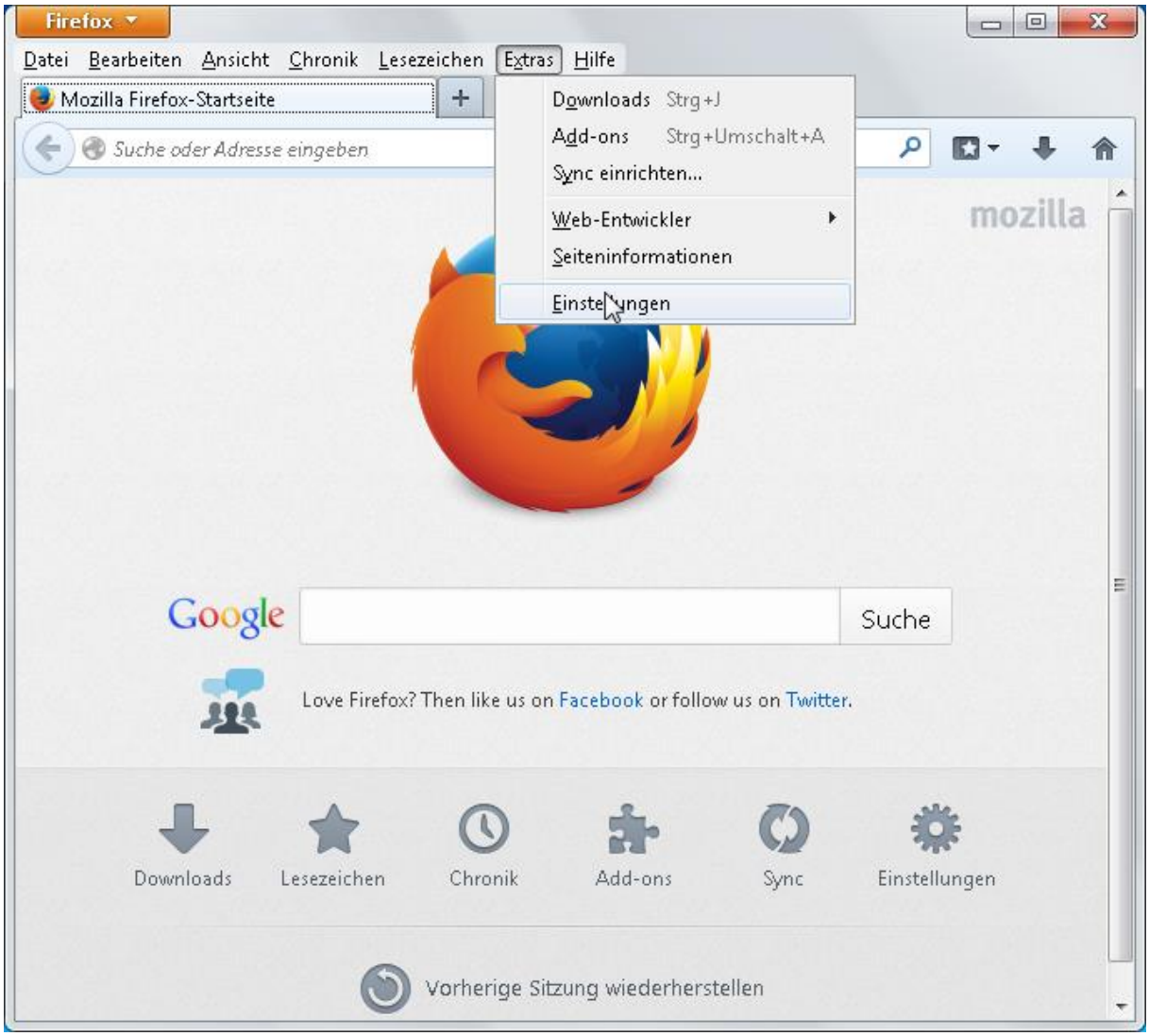

Sie nehmen Änderungen an Ihren Systemeinstellungen für Zertifizierungen vor. Geben Sie Ihr Kennwort ein, um dies zu erlauben.
Name: your-user
Kennwort:
Abbrechen
Einstellungen aktualisieren

Das Zertifikat ist nun eingerichtet.

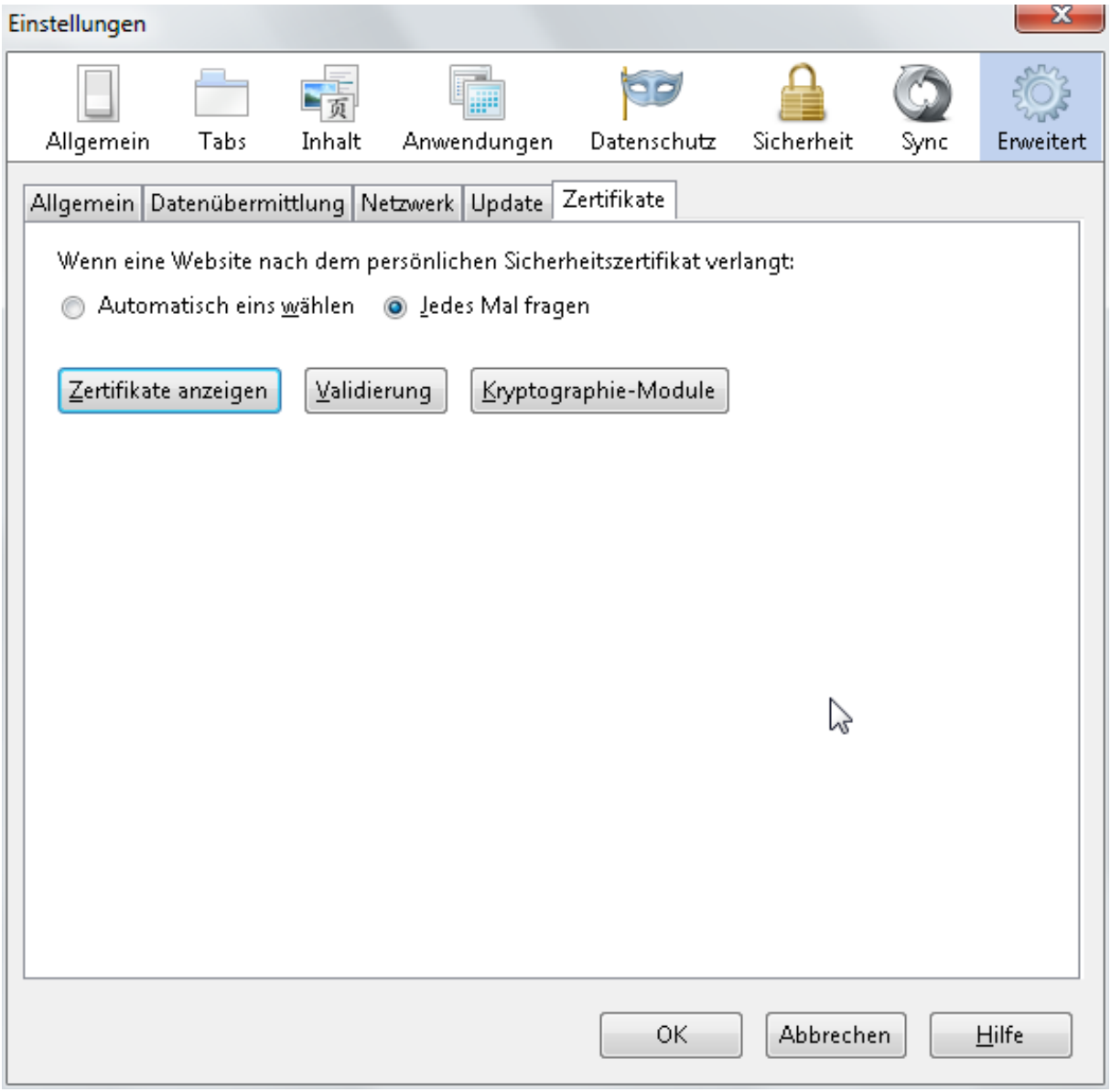
Zertifikat in Firefox einrichten

Das Einrichten des Zertifikats in Firefox ist in allen Betriebssystemen ähnlich. Schauen wir es uns am Beispiel von MS Windows an.

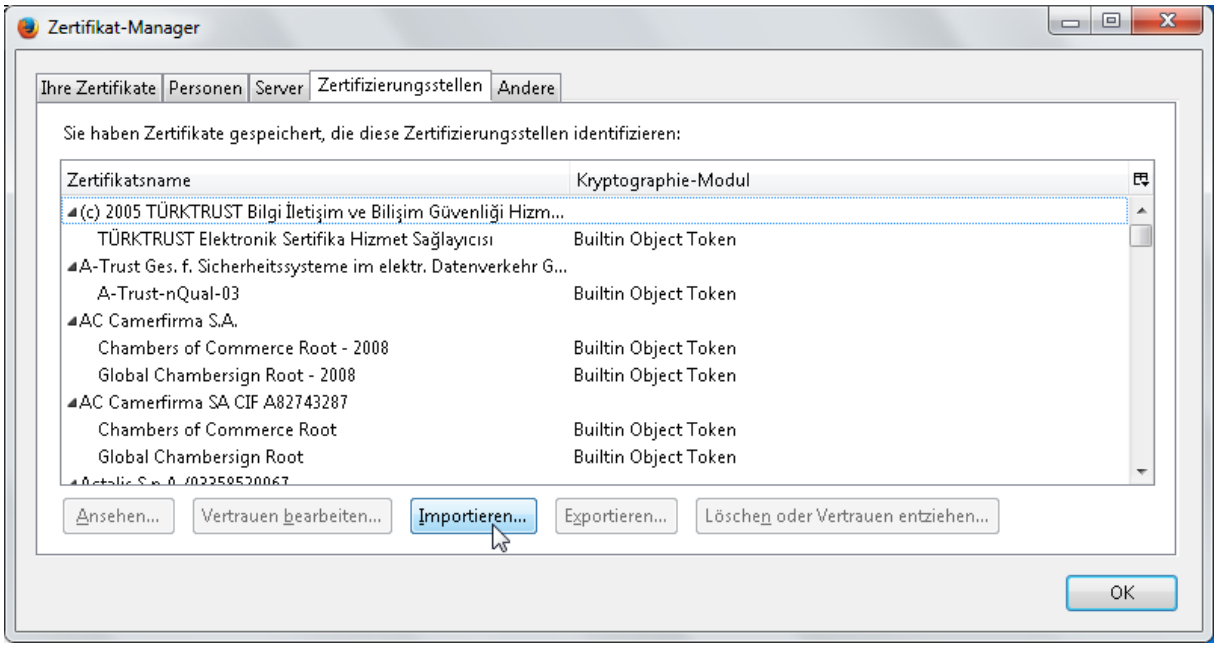
Öffnen Sie die Einstellungen von Firefox (**Extras->Einstellungen**):

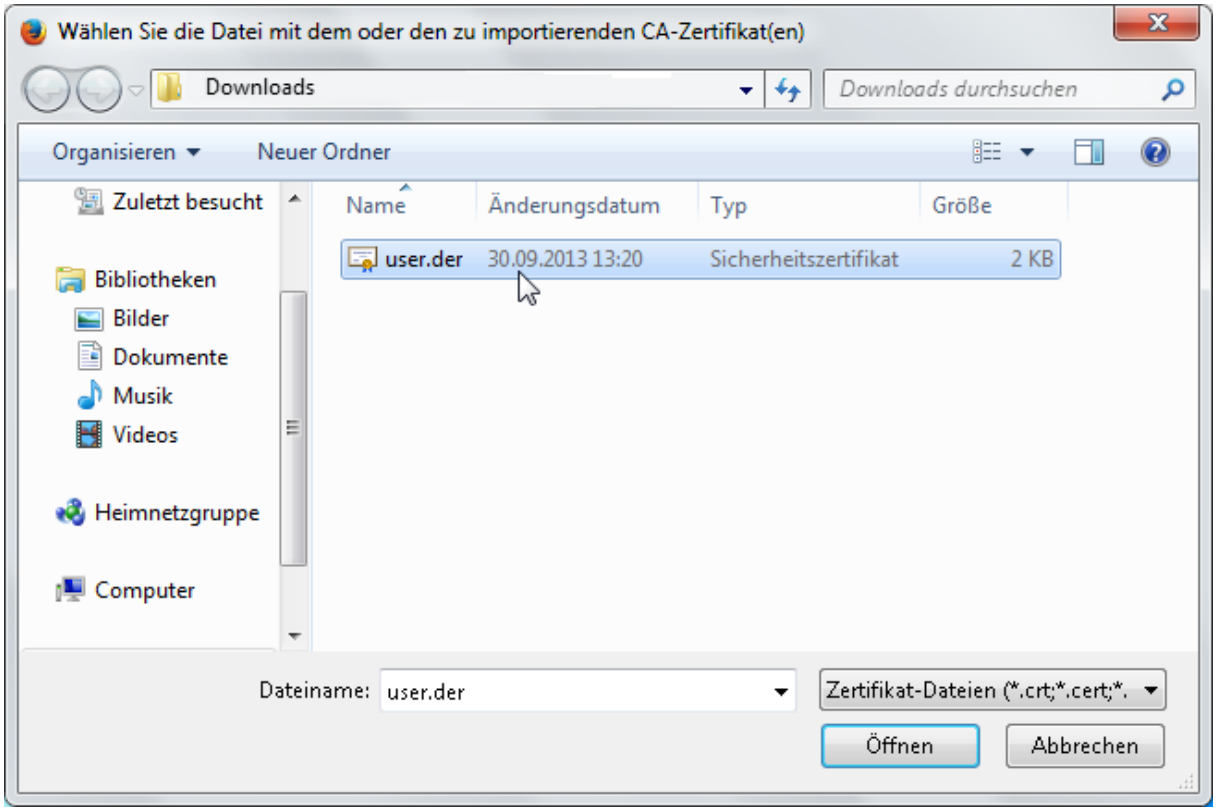


Gehen Sie zu **Erweitert** und wählen Sie den Reiter **Zertifikate**. Klicken Sie auf die Schaltfläche **Zertifikate anzeigen**:

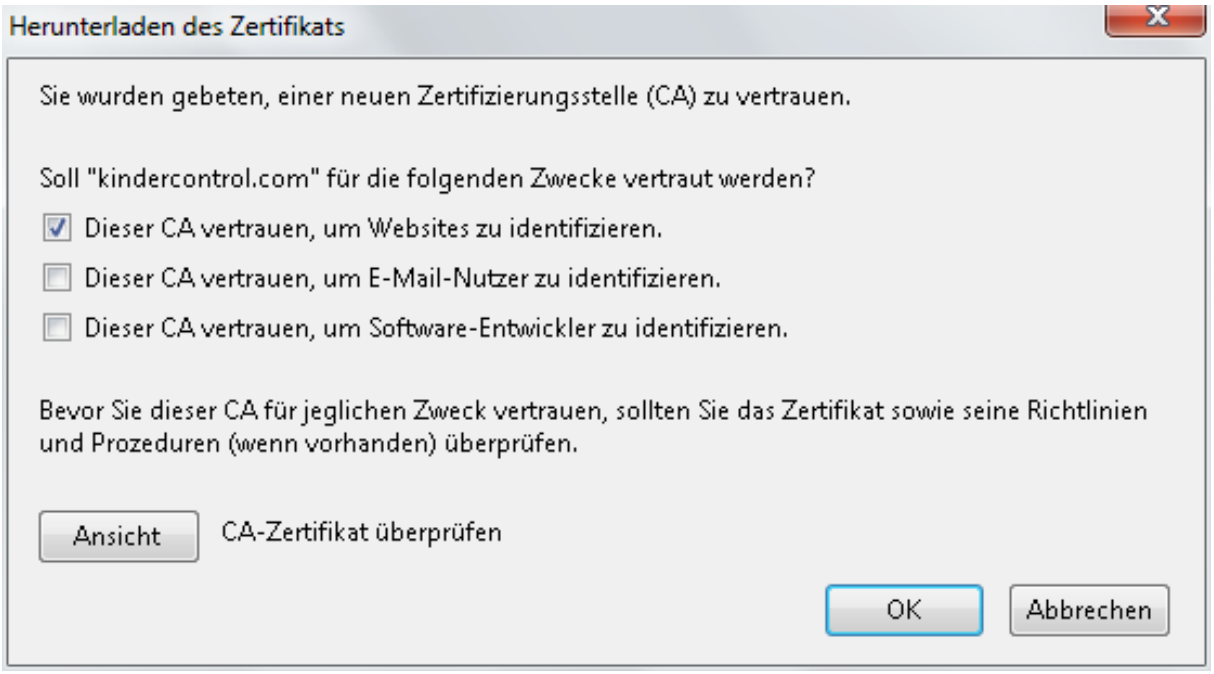


Klicken Sie auf die Schaltfläche „Importieren“ und geben Sie den Pfad zum Zertifikat ein (Datei user.der):





Setzen Sie ein Häkchen neben **Diesem CA vertrauen, um Websites zu identifizieren** und klicken Sie auf **OK**:


Herunterladen des Zertifikats
Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.
Soll "kindercontrol.com" für die folgenden Zwecke vertraut werden?
Dieser CA vertrauen, um Websites zu identifizieren.
Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.
Dieser CA vertrauen, um Software-Entwickler zu identifizieren.
Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien und Prozeduren (wenn vorhanden) überprüfen.
Ansicht
CA-Zertifikat überprüfen
OK
Abbrechen

Das Einrichten des Zertifikats ist nun abgeschlossen.